(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3784423号
(P3784423)
(45)発行日　平成18年6月14日(2006.6.14)　(24)登録日　平成18年3月24日(2006.3.24)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 550G
H04L 9/10 (2006.01)　　G06F 9/06 550C
　　H04L 9/00 621Z

請求項の数 32　(全 31 頁)

(21)出願番号　特願平5-113157
(22)出願日　平成5年5月14日(1993.5.14)
(65)公開番号　特開平6-103058
(43)公開日　平成6年4月15日(1994.4.15)
審査請求日　平成12年5月2日(2000.5.2)
審判番号　不服2003-12732(P2003-12732/J1)
審判請求日　平成15年7月4日(2003.7.4)
(31)優先権主張番号　883867
(32)優先日　平成4年5月15日(1992.5.15)
(33)優先権主張国　米国(US)
(31)優先権主張番号　883868
(32)優先日　平成4年5月15日(1992.5.15)
(33)優先権主張国　米国(US)

(73)特許権者　593067033
アディソン・エム・フィッシャー
ＡＤＤＩＳＯＮ　Ｍ.　ＦＩＳＣＨＥＲ
アメリカ合衆国、３３９４２　フロリダ州、ナプルズ、フォーティーンス・アベニュ・サウス、６０
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100096781
弁理士　堀井　豊

最終頁に続く

(54)【発明の名称】データセキュリティのための改良された方法、およびコンピュータシステム

(57)【特許請求の範囲】

【請求項１】

複数のプログラムを実行するための処理手段（２）と、少なくとも１つのプログラムを記憶するためのメモリ手段（７）とを含むコンピュータシステムにおいて、データセキュリティのための改良された方法は、

何の権限がプログラムに割当てられるべきであるかをユーザに尋ね、関連のプログラムによって使用される少なくとも１つのそれらのコンピュータ資源および機能を示す複数の権限エントリを記憶するための、プログラム権限情報（図２）を組立てるステップと、

前記メモリ手段に前記プログラム権限情報を記録する（２７２）ステップと、

プログラム権限情報を、前記コンピュータシステムによって実行されるべき少なくとも１つのプログラムに関連させ（２７２）、それによってプログラム権限情報をその関連のプログラムが前記処理手段によって実行されるとき調査し（３４０）、前記プログラム権限情報が機能／資源を許容するかを判定し（３４２）、許容する時に機能を実行するステップ（３５４）とを前記処理手段に実行させる、改良された方法。

【請求項２】

プログラム権限情報の一部として実行されるべき前記プログラムのディジタルハッシュ（２４）を提供するステップをさらに含む、請求項１に記載の方法。

【請求項３】

権限エンティティのプライベートキーでプログラム権限情報の少なくとも一部にディジタル署名するステップをさらに含む、請求項１に記載の方法。

【請求項４】

ディジタル署名するステップは、複数のディジタル署名がいかなるディジタル署名も有効であるために要求されるということを示す（４４）ことを含む、請求項３に記載の方法。

【請求項５】

ディジタル署名するステップは、ディジタル署名を行なうものに認められている権限の少なくとも１つの資格付けを示す（４０）ステップを含む、請求項３に記載の方法。

【請求項６】

プログラム権限情報は関連のプログラムが実行される前にコンピュータユーザによって確立される、請求項１に記載の方法。

【請求項７】

特別な特権を有さないユーザ自身の使用のために前記プログラム権限情報を確立する、請求項６に記載の方法。

【請求項８】

何の権限がプログラムに割当てられるべきであるかをユーザに尋ね、前記プログラム権限情報を組立てるステップでは、プログラムがアクセスを有し得る少なくとも１つのデータファイルの少なくとも一部の指示を尋ねてプログラム権限情報を組立てる、請求項１に記載の方法。

【請求項９】

組立てるステップでは、実行されるべきプログラムがアクセスを有する少なくとも１つのファイルの指示を与え、かつ少なくとも１つのファイルに情報を書込む能力を特定する（２１６）、請求項１に記載の方法。

【請求項１０】

組立てるステップでは、前記プログラムによって呼出される権限を付与されるプログラムの組の指示を与える、請求項１に記載の方法。

【請求項１１】

実行されるべきプログラムと関連する前記記憶されたプログラム権限情報を使用して、少なくとも１つのリソースおよび機能の使用を制限するステップをさらに含む、請求項１に記載の方法。

【請求項１２】

組立てるステップでは、情報を伝送する前記関連のプログラムの権限を支配する少なくとも１つの規則を示す（２２６）、請求項１に記載の方法。

【請求項１３】

少なくとも１つの規則は、情報を伝送する権限に電子郵便を利用することが含まれることを規定する（２２２）、請求項１２に記載の方法。

【請求項１４】

組立てるステップでは、プログラムがディジタル署名を行なうことができるかどうかを管理する少なくとも１つの規則を与える、請求項１に記載の方法。

【請求項１５】

組立てるステップでは、プログラムが文書開放動作を行なうことができるかどうかを管理する、請求項１に記載の方法。

【請求項１６】

組立てるステップでは、プログラムが権限によって十分な監視を受けていない機械語命令を実行することができるかどうかを管理する、請求項１に記載の方法。

【請求項１７】

組立てるステップでは、前記関連のプログラムがアクセスすることを許容されるメモリの組を資格付けする（２１２、２１６）、請求項１に記載の方法。

【請求項１８】

組立てるステップでは、ユーザへ情報を表示するプログラムの能力を支配する資格付けの組を示す（２３８）、請求項１に記載の方法。

【請求項１９】

組立てるステップでは、ユーザから情報を請求するプログラムの能力を支配する資格付けの組を示す（２４２）、請求項１に記載の方法。

【請求項２０】

組立てるステップでは、コンピュータへ結合されるコンピュータ制御されたリソースを制御するプログラムの能力を支配する資格付けの組を示す（２５０）、請求項１に記載の方法。

【請求項２１】

資格付けの組はモデムを介して情報を伝送するプログラムの能力を支配する、請求項２０に記載の方法。

【請求項２２】

複数のプログラムを実行するための実行手段と、前記実行手段へ結合され、データおよびプログラム命令を記憶するためのメモリ手段とを有するコンピュータシステムにおいて、コンピュータユーザのために前記実行手段によってプログラムを実行するための方法は、

前記実行手段が、実行されるべきプログラムを識別するステップ（３００）と、

プログラム権限情報がプログラムと関連しているか否かを前記実行手段が決定するステップ（３０４）とを含み、前記プログラム権限情報は、前記コンピュータユーザが利用可能である実行操作に基づいてプログラムに能力を与え、

前記実行手段が、前記プログラム権限情報を、調査するステップ（３４０）と、

前記実行手段が、関連のプログラムが企図された動作を実行することを許容されるか否か、前記プログラム権限情報の調査から決定するステップ（３４２）と、

もし前記プログラム権限情報が、前記プログラムが企図された動作を実行することを許容されないことを示せば、前記実行手段が、前記動作を抑制するステップ（３４４、４１０）とをさらに含む、方法。

【請求項２３】

前記プログラムが要求されたリソースを利用することを許可されて
いるかどうか判断するために、前記プログラム権限情報をチェックするステップをさらに含む、請求項２２に記載の方法。

【請求項２４】

前記プログラム権限情報が前記関連のプログラムで規定される動作を許容するか否かをチェックするステップをさらに含む、請求項２２に記載の方法。

【請求項２５】

ユーザが予め定められた動作を行なうプログラムを実行する権限を割当てられているか否かを決定するためにチェックを行なうステップ（３４６）をさらに含む、請求項２２に記載の方法。

【請求項２６】

前記プログラム権限情報に関連するいかなるディジタル署名も確証するステップ（３１６）をさらに含む、請求項２２に記載の方法。

【請求項２７】

もし前記ディジタル署名が有効でなければ、前記プログラムの実行を抑制するためのステップ（３２２、３２４）を含む、請求項２６に記載の方法。

【請求項２８】

前記プログラム権限情報は前記プログラムのハッシュを記憶するための部分を含み、前記プログラムのハッシュを計算し、計算されたハッシュを前記記憶されたハッシュと比較するステップをさらに含む、請求項２２に記載の方法。

【請求項２９】

ディジタル署名の署名者と関連する権限を確証するステップ（３０８）をさらに含む、請求項２２に記載の方法。

【請求項３０】

前記プログラム権限情報は前記関連のプログラムがアクセスする権限を有するデータの組の指示を含む、請求項２２に記載の方法。

【請求項３１】

前記プログラム命令は機械語コードで表され、前記動作はプログラム権限情報を監視し、強化する、管理されたスーパバイザへの呼出しを介して行なわれる、請求項２２に記載の方法。

【請求項３２】

前記プログラム命令は、前記プログラム権限情報を監視し、強化するインタプリタプログラムによって処理される解釈「疑似」コードで表される、請求項２２に記載の方法。

【発明の詳細な説明】

【０００１】

【発明の分野】

この発明は一般にディジタル情報に向上したセキュリ

ティおよび保護を与えるための方法および装置に関する。より特定的に、この発明はユーザ間で送信されるコンピュータプログラム、特に出所が不明のプログラムを処理する一方で、向上されたコンピュータシステムセキュリティを与えるための方法および装置に関する。

【０００２】

【発明の背景および概要】

コンピュータ「ウィルス」の潜在的に破壊的な結果は広く一般に知られてきた。コンピュータウィルスは、実行された場合に、ユーザが予期した動作だけではなく、プログラムに組込まれた予期しない、しばしば破壊的な動作の実行を結果としてもたらすコンピュータプログラムという視点から見られるかもしれない。コンピュータウィルスはまた、実行された場合に、そのコードの一部を取出して、そのようなコードを他のプログラムに置いてそれによって他のプログラムを感染させるプログラムという視点から見られるかもしれない。ウィルスはシステム内の他のプログラムを変更し、システムに様々なトラップを設定し、様々なコントロールプログラムを変え、システムのファイルを消去またはそうでない場合には変更などするかもしれない。

【０００３】

このようなウィルスはユーザのデータを予期しない方法で損なう、調べるまたは傷をつける望ましくない副作用を有するように典型的に悪意をもって構成される。コンピュータウィルスに伴う問題は、ウィルス制御プログラムがユーザがある必要なデータにアクセスした場合に「暗黙のうちに」典型的に実行され、その結果ユーザは破壊的なプログラムが実行されていることに気づきさえしないという事実によって、しばしばよりひどいものになる。

【０００４】

この発明はこのようなウィルスからの、およびシステムに基づいて実行するが実際のコンピュータウィルスキャリアではないプログラムからの、保護を提供する。この点に関して、プログラムはコンピュータシステムおよび／または関連データに意図しない逆影響を有し得る。たとえば、実行プログラムはあるユーザデータが第三者に送られることを不注意に引起こし得る。このようなプログラムはプログラミングエラーの結果であったかもしれないし、または特定の問題を生じるように故意に設計されたものであるかもしれない。

【０００５】

先行技術の動作システムはデータをコンピュータユーザから保護するように典型的に設計される。このようなシステムでは、ユーザはしばしば様々な権限を割当てられ、その後関連権限に基づいてプログラムを実行することが可能である。もしユーザの割当てられた権限を超えるプログラムが実行されていれば、そのようなシステムはそのプログラムの実行を停止させるであろう。このよ

うな先行技術のシステムは、コンピュータウィルスなどからコンピュータユーザを適切に保護しない。

【０００６】

ある「システム」関連ファイルをプログラムによって変更されることから保護するセキュリティシステムがある。しかしながら、このようなシステムはコンピュータユーザをユーザ自身のファイルを実行し変更するプログラムから典型的に保護しない。

【０００７】

この発明はユーザ間で送信される、それ自身のプログラム命令を含む、複雑なデータ構造、たとえば、オブジェクトを伴って動作する場合でさえ、信頼できるセキュリティを提供することに向けられる。この発明はまたシステムプログラムまたはデータをコンピュータウィルスまたはできの悪いプログラミングの潜在的に壊滅的な結果にさらすことなく、より従来的なプログラム、たとえばコンピュータ掲示板からの出所の不確かなものをも処理する場合に、向上したセキュリティを提供する。

【０００８】

この発明の方法および装置は、まさに実行されようとしているプログラムの能力を、予め規定された資源の使用（たとえばデータファイル、データ書込み能力など）に制限するシステムモニタを含む独自の動作システム設計を利用する。このシステムモニタはどのプログラムが実行を許可され、および／またはどのプログラムが実行から除外されるかを規定する１組の権限を含むプログラム権限情報を構築する。

【０００９】

実行されるべきプログラムに割当てられた権限および／または制限の組をここで「プログラム権限情報」（または「ＰＡＩ」）と呼ぶ。一旦規定されると、プログラム権限情報はその後実行されるべき各プログラムと関連して、それによってプログラムが利用することを許可される資源および機能のタイプを正確に表わす。特定のプログラムに関連するＰＡＩは、コンピュータシステムオーナ／ユーザによって、またはそのコンピュータシステムオーナ／ユーザが絶対的に信用する誰かによって割当てられ得る。

【００１０】

ＰＡＩはプログラムが実行し得る動作の範囲を規定し、および／またはプログラムが実行できない動作を規定する。このプログラムは権限を与えられたものにアクセスすることを許可されるが、それ以外には何もアクセスすることができない。この態様で、プログラムはプログラム能力制限「セーフティボックス」に置かれているものとみなされ得る。この「セーフティボックス」はシステムモニタがプログラムを実行するときはいつでも、そのプログラムのためのＰＡＩが同様にロードされかつモニタされるように、その後プログラムと関連づけられる。プログラムが機能を実行しようとする、または資源に

アクセスしようとする場合には、関連するＰＡＩがその動作が規定されたプログラム制限内であることを確認するためにモニタされる。もしプログラムが権限を付与された制限の範囲を超えて何かを実行しようとすれば、プログラム実行は停止される。

【００１１】

このように、この発明は実行されるべき任意のプログラムからユーザを有利に保護する。この発明は、プログラムがコンピュータ掲示板または不明の信用性を有する他のユーザのような広い範囲の異なった信頼できない場所から得られる、現在のデータ処理実務に鑑みて特に有利である。

【００１２】

この発明は上述のＰＡＩがプログラムそれ自体（またはプログラムのハッシュ）とともに、ユーザが信用するあるエンティティによってディジタル署名され得ることを熟慮する。ディジタル署名がＰＡＩを有効にするために使用された場合、前述のＰＡＩモニタリングはＰＡＩ上のディジタル署名を確証して、それがユーザによって信用されるエンティティに属するものであること、それが適切に権限を付与されていること、およびそれならびにその関連プログラムが手を加えられなかったことを確実にすることを含む。

【００１３】

この発明は本発明者の米国特許第 4,868,877号および第 5,005,200号に記載されたような階層信用ディジタル署名証明システムの使用を熟慮するものであり、これらの特許は引用によりここに援用される。これらの特許の教示に従って、単一のハイレベル権限付与エンティティが安全に権限を委任し、多数の他のエンティティの間でプログラムに権限を付与し、かつ任意のレベルで共同署名を要求することが可能であり、それによって権限付与主体（agent）自身によるエラー、不正の可能性を禁止する。これは単一のソフトウェア認証グループが大人口にサービスすることを可能にし、それによって各ユーザに対する１人当たりの費用を大幅に削減する。

【００１４】

この発明の１つの熟慮された実施例において、プログラムはデータオブジェクトの一部であってもよく、それは高級制御言語で書かれ、この高級言語を実行する標準化されたインタプリタプログラムによって実行される。この場合、インタプリタのタスクの一部は、高級論理で遇隅される機能は実際は許可されることを確証することである。もしこのようなタスクが許可されなければ、インタプリタはそのようなタスクを実行する権限が付与されていないプログラムの実行を抑制する。

【００１５】

多くの利点がこの発明の使用から生じる。たとえば、この発明は隠されたプログラムまたはウィルスがシステムに導入されることが不可能になるように、プログラム

に制限を結びつける役割を有利に果たす。ユーザは、１つの機能のために意図されたプログラムが、（コンピュータウィルスの広がりをもたらすように）偶然または故意に渡っていき、他の関連のないまたは重要な資源に影響を及ぼすことがないことを確実にするために、実行され得る機能に関する詳細を特定することによって保護される。ここに記載された態様におけるプログラム権限情報の使用によって、ユーザは自分が実行するプログラムから自分自身を保護することが可能である。

【００１６】

管理主体はプログラムの論理のすべての局面を理解する必要性を伴わずに、プログラムの範囲を効果的に制限することができる。管理人はその意図した機能および定義に基づいてプログラムに権限を付与しかつ制限することが可能であり、それによってプログラム欠陥の危険を軽減させる。この態様で、ソフトウェア「時限爆弾」またはウィルスを植えつけようとするかもしれない乱心したまたはいたずら半分のプログラマーの危険は制限され得る。

【００１７】

この発明はまたディジタル署名がＰＡＩを確証することを可能にする。このように、プログラムは、すべてのメンバーが共通の高級署名権限を信用している大人口の間で、自由にかつ安全に交換可能である。

【００１８】

不明の信用性を有するプログラムでさえ、プログラム権限情報が広い範囲の制限を関連づけて、それによって潜在的に有益なプログラムが安全に使用されることを許容した後、たとえ公式の信用証明を持っていなくても、使用することが可能である。

【００１９】

この発明はまた無限の数の異なった資源および機能が制御されることを可能にする。たとえば、制御され得るいくつかの有用な資源／機能は、プログラムをあるファイルまたはデータセットに制限する能力、電子メールを経てユーザの支配領域の範囲の外にいる誰かにデータを送信する能力、ディジタル署名を作るまたは要求するプログラムの能力、あるセキュリティクラスのプログラムへのアクセスを制限する能力などを含む。

【００２０】

この発明はまたプログラムがディジタル署名動作を実行することができるかどうかを制限し、かつどのようにそのような署名が実行されるべきかを制限する能力を提供する。多くの場合、プログラムがユーザからのディジタル署名を求めることに巻込まれた場合、その署名が与えられようとしているデータをユーザに承知させるかどうかはプログラム次第である。電子データ交換（ＥＤＩ）トランザクションの場合にそのようである。この場合、いたずら半分のアプリケーションプログラムが、ユーザに１組のデータを見せ、しかも他の組のデータを署名のために送ることは考えられることである。この場合、そのプログラムはユーザを騙してユーザが信じるように仕向けられたものとは完全に異なった情報にディジタル署名させたことになる。この発明はユーザをディジタル署名を求めるプログラムから保護するメカニズムを提供する。

【００２１】

この発明を使用することによって、一般的なオブジェクト指向データは、ユーザをウィルスまたはいたずら半分のユーザの潜在的な危険にさらすことなく、ユーザ間で転送され得る。

【００２２】

この発明のある局面に従うと、プログラムは、複数のプログラムを実行するための処理手段（２）と、プログラム命令およびデータを記憶するためのメモリ手段（７）とを有するコンピュータシステムを、プログラム権限情報を用いて動作させるためのプログラムであって、前記メモリ手段に、複数の権限エントリ（３２、３４、３６）を記憶するためのステップをコンピュータに実行させ、前記権限エントリは関連のプログラムが実行することを許容する動作を資格付け、少なくとも１つのセグメントに、前記権限エントリを少なくとも１つのプログラム（１１２、１５３）と関連させるためのデータを記憶するためのステップをコンピュータに実行させ、前記複数の権限エントリを記憶するためのステップは、前記エントリ（３４）の各々について少なくとも１つの機能およびリソースのタイプを示すためのステップを含む。

【００２３】

好ましくは、前記少なくとも１つのセグメントは前記関連のプログラム（２４）のハッシュを記憶するための部分を含む。

【００２４】

好ましくは複数の権限エントリを記憶するためのステップはプログラムに対して認められている権限および能力の資格付けを記憶するためのステップを含む。

【００２５】

好ましくはプログラムは、ディジタル署名（４０）を記憶するためのステップをさらに含む。

【００２６】

好ましくはプログラムは、署名する当事者に対して認められる権限を示すためのステップをさらに含む。

【００２７】

好ましくはプログラムは、複数のディジタル署名が有効とみなされるべき少なくとも１つの署名について必要であることを示すためのステップをさらに含む。

【００２８】

好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムがアクセスする権限を有するデータの組の指示を記憶するためのステップを含む。

【００２９】
好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムがアクセスする権限を有する少なくとも１つのファイルのフィールドの組の指示（３２，３６，４６のいずれか）を記憶するためのステップを含む。
【００３０】
好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムがプログラムを呼出す権限を有するか否かの指示（２１０）を記憶するためのステップを含む。
【００３１】
好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムが電子郵便を生成する権限を有するか否かの指示（２２２）を記憶するためのステップを含む。
【００３２】
好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムがデータを他のユーザへ伝送する権限を有するか否かの指示（２２６）を記憶するためのステップを含む。
【００３３】
好ましくは、複数の権限エントリを記憶するための前記ステップは、前記関連のプログラムが文書開放動作を行なう権限を有するか否かの指示（２２８）を記憶するためのステップを含む。
【００３４】
好ましくは、複数の権限エントリを記憶するための前記ステップは、メモリアクセス特権がこのプログラムで権限付与されたという指示（２３２）を記憶するためのステップを含む。
【００３５】
好ましくは、複数の権限エントリを記憶するための前記ステップは、ユーザへ情報を表示する能力に関する前記関連のプログラムの少なくとも１つの修飾の指示（２３８）を記憶するためのステップを含む。
【００３６】
好ましくは、複数の権限エントリを記憶するための前記ステップは、ユーザのために入力を請求する能力に関して前記関連のプログラムにおける少なくとも１つの資格付けの指示（２４７）を記憶するためのステップを含む。
【００３７】
好ましくは、複数の権限エントリを記憶するための前記ステップは、ユーザのためにディジタル署名を請求する能力に関して前記関連のプログラムにおける少なくとも１つの資格付けの指示（２４６）を記憶するためのステップを含む。
【００３８】
好ましくは複数の権限エントリを記憶するための前記

ステップは、装置を制御する能力に関して前記関連のプログラムにおける少なくとも１つの資格付けの指示（２５０）を記憶するためのステップを含む。
【００３９】
好ましくは複数の権限エントリを記憶するための前記ステップは、アクセスがセキュリティクリアランスによって制限されることの指示を記憶するためのステップを含む。
【００４０】
好ましくは記憶するための前記ステップは、文書開放動作が行なわれてもよいという指示を記憶するためのステップを含む。
【００４１】
好ましくは前記複数の権限エントリはディジタル署名の一部として含まれる。
【００４２】
この発明の他の局面に従うと、複数のプログラムを実行するための処理手段（２）と、少なくとも１つのプログラムを記憶するためのメモリ手段（７）とを含むコンピュータシステムにおいて、データセキュリティのための改良された方法は、関連のプログラムによって使用されるであろう少なくとも１つのそれらのコンピュータ資源および機能を示す複数の権限エントリを記憶するための、確立されたプログラム権限情報（図２）を入力するステップと、前記メモリ手段に前記プログラム権限情報を格納する（２６６）ステップと、プログラム権限情報を、前記コンピュータシステムによって実行されるべき少なくとも１つのプログラムに関連させ、それによってプログラム権限情報がその関連のプログラムが実行されるとき監視される（２７２）ステップとを前記処理手段に実行させる。
【００４３】
好ましくは方法は、プログラム権限情報の一部として実行されるべき前記プログラムのディジタルハッシュ（２４）を提供するステップをさらに含む。
【００４４】
好ましくは方法は、権限エンティティのプライベートキーでプログラム権限情報データの少なくとも一部にディジタル署名するステップをさらに含む。
【００４５】
好ましくはディジタル署名するステップは、複数のディジタル署名がいかなるディジタル署名も有効であるために要求されるということを示す（４４）ことを含む。
【００４６】
好ましくはディジタル署名するステップは、ディジタル署名を行なうものに認められている権限の少なくとも１つの資格付けを示す（４０）ステップを含む。
【００４７】
好ましくはプログラム権限情報は関連のプログラムが実行される前にコンピュータユーザによって確立される

。

【００４８】

好ましくは方法は、特別な特権を有さないユーザ自身の使用のために前記プログラム権限情報を確立する。

【００４９】

好ましくは確立するステップは、プログラムがアクセスを有し得る少なくとも１つのデータファイルの少なくとも一部の指示（２１２）を与える。

【００５０】

好ましくは確立するステップは、実行されるべきプログラムがアクセスを有する少なくとも１つのファイルの指示を与え、かつ少なくとも１つのファイルに情報を書込む能力を特定する（２１６）。

【００５１】

好ましくは確立するステップは、前記プログラムによって呼出される権限を付与されるプログラムの組の指示（２２０）を与える。

【００５２】

好ましくは方法は、実行されるべきプログラムと関連する前記記憶されたプログラム権限情報を使用して、少なくとも１つのリソースおよび機能の使用を制限するステップをさらに含む。

【００５３】

好ましくは確立するステップは、情報を伝送する前記関連のプログラムの権限を支配する少なくとも１つの規則を示す（２２６）。

【００５４】

好ましくは少なくとも１つの規則は、情報を伝送する権限に電子郵便を利用するステップが含まれることを規定する（２２２）。

【００５５】

好ましくは確立するステップは、プログラムがディジタル署名を行なうことができるかどうかを管理する少なくとも１つの規則を与える。

【００５６】

好ましくは確立するステップは、プログラムが文書開放動作を行なうことができるかどうかを管理する。

【００５７】

好ましくは確立するステップは、プログラムが権限によって十分な監視を受けていない機械語命令を実行することができるかどうかを管理する。

【００５８】

好ましくは確立するステップは、前記関連のプログラムがアクセスすることを許容されるメモリの組を資格付けする（２１２、２１６）。

【００５９】

好ましくは確立するステップは、ユーザへ情報を表示するプログラムの能力を支配する資格付けの組を示す（２３８）。

【００６０】

好ましくは確立するステップは、ユーザから情報を請求するプログラムの能力を支配する資格付けの組を示す（２４２）。

【００６１】

好ましくは確立するステップは、コンピュータへ結合されるコンピュータ制御されたリソースを制御するプログラムの能力を支配する資格付けの組を示す（２５０）。

【００６２】

好ましくは資格付けの組はモデムを介して情報を伝送するプログラムの能力を支配する。

【００６３】

この発明の他の局面に従うと、複数のプログラムを実行するための実行手段と、前記実行手段へ結合され、データおよびプログラム命令を記憶するためのメモリ手段とを有するコンピュータシステムにおいて、コンピュータユーザのために前記実行手段によってプログラムを実行するための方法は、前記実行手段が、実行されるべきプログラムを識別するステップ（３００）と、プログラム権限情報がプログラムと関連しているか否かを前記実行手段が決定するステップ（３０４）とを含み、前記プログラム権限情報は前記コンピュータユーザが利用可能である実行操作からプログラムに能力を与え、前記実行手段が、前記プログラム権限情報を、調べるステップ（３１０、３３０）と、前記実行手段が、関連のプログラムが企図された動作を実行することを許容されるか否か、前記プログラム権限情報の調査から決定するステップ（３４２）と、もし前記プログラム権限情報が、前記プログラムが企図された動作を実行することを許容されないことを示せば、前記実行手段が、前記動作を抑制するステップ（３４４、４１０）とをさらに含む。

【００６４】

好ましくは方法は、前記プログラムが要求されたリソースを利用することを許可されているかどうか判断するために、前記権限情報をチェックするステップをさらに含む。

【００６５】

好ましくは方法は、前記プログラム権限情報が前記関連のプログラムで規定される動作の性能を許容するか否かをチェックするステップをさらに含む。

【００６６】

好ましくは方法は、ユーザが予め定められた動作を行なうプログラムを実行する権限を割当てられているか否かを決定するためにチェックを行なうステップ（３４６）をさらに含む。

【００６７】

好ましくは方法は、前記プログラム権限情報に関連するいかなるディジタル署名も確証するステップ（３１６）をさらに含む。

【００６８】

好ましくは方法は、もし前記ディジタル署名が有効でなければ、前記プログラムの実行を抑制するためのステップ（３２２、３２４）を含む。

【００６９】

好ましくは方法は、前記プログラムの権限情報を前記プログラムを呼出しているルーチンに関連する権限情報と組合わせるステップをさらに含む。

【００７０】

好ましくは前記権限情報は前記プログラムのハッシュを記憶するための部分を含み、方法は、前記プログラムのハッシュを計算し、計算されたハッシュを前記記憶されたハッシュと比較するステップをさらに含む。

【００７１】

好ましくは方法は、ディジタル署名の署名者と関連する権限を確証するステップ（３０８）をさらに含む。

【００７２】

好ましくは方法は、前記プログラムの権限情報を、前記プログラムによって呼出されるルーチンと関連する権限情報と組合わせるステップをさらに含む。

【００７３】

好ましくは、前記権限情報は前記関連のプログラムがアクセスする権限を有するデータの組の指示を含む。

【００７４】

好ましくは前記プログラム命令は機械語コードで表され、前記動作はプログラム権限情報を監視し、強化する、管理されたスーパバイザへの呼出しを介して行なわれる。

【００７５】

好ましくは方法は、前記プログラム権限情報を、自身を別の行先へ伝送するための命令を含む移動プログラムと関連させるステップをさらに含む。

【００７６】

好ましくは方法は、証明を変数として、前記変数が前記プログラムによって演算され得るような移動プログラム内に記憶するステップをさらに含む。

【００７７】

好ましくは前記プログラム命令は、前記プログラム権限情報を監視し、強化するインタプリタプログラムによって処理される解釈「疑似」コードで表される。

【００７８】

この発明のこれらおよび他の特徴は、添付の図面とともに考えられるこの発明の好ましい実施例の以下の説明を読むことによってよりよく理解されるであろう。

【００７９】

【実施例の詳細な説明】

図１はこの発明とともに使用され得る例証的なコミュニケーションシステムをブロック図形式で示す。このシステムはコミュニケーションチャンネル１２を含み、それはたとえばそれを介して端末Ａ、Ｂ、…Ｎ間のコミュニケーションが行なわれ得る安全にされていないチャンネルであってもよい。コミュニケーションチャンネル１２はたとえば電話線であってもよい。端末Ａ、Ｂ、…Ｎは、ほんの一例として、従来のキーボード／ＣＲＴディスプレイ４に結合されるプロセッサ（メインメモリを有する）２を有するＩＢＭ　ＰＣであってもよい。付加的に、各プロセッサは不揮発性プログラムおよびディスクメモリデバイスであり得るプログラム権限情報（ＰＡＩ）記憶（storage）７に好ましくは結合される。各端末Ａ、Ｂ、…Ｎはまた従来のＩＢＭコミュニケーションボード（図示せず）を含み、それは従来のモデム６、８、１０にそれぞれ結合された場合、端末がメッセージを送受信することを可能にする。

【００８０】

各端末はディジタル署名動作が要求されることであれば何でも実行するメッセージを発生し、かつそのメッセージをコミュニケーションチャンネル１２（またはコミュニケーションチャンネル１２に接続され得るコミュニケーションネットワーク（図示せず））に接続される他の端末のいずれにもそのメッセージを送信することが可能である。端末Ａ、Ｂ…Ｎはまた、要求された各メッセージに対して署名確証を実行することが可能である。

【００８１】

図２は例証的なプログラム権限情報（ＰＡＩ）のデータ構造の例示である。ＰＡＩは１組の権限付与仕様セグメント２２－３８、および１組の権限付与署名セグメント４０－４８（ある状況ではオプションであってもよい）を含む。

【００８２】

ヘッダセグメント２０は権限付与仕様セグメントに先行し、後に続くプログラム権限情報の長さを規定する。フィールド長情報はプログラマーがメモリの関連権限情報の程度を容易に決定することを許容する。このように、もし、たとえばオブジェクト指向データ構造（図５に関連して以下に説明される）が利用可能であれば、フィールド２０はプログラム権限情報セグメント１１６が終了するポイントを識別して、図５に示されるプログラムセグメント１１８の位置を突き止める役割を果たすであろう。

【００８３】

セグメント２２および２４は「ハッシュ」関連セグメントである。当業者によって理解されるように、「ハッシュ」は「一方向」機能であり、同一の値にハッシュする２つのデータ値を見つけることは計算では実行不可能である。すべての実務的な目的のために、ハッシュ関数をデータのオリジナル集合に適用することから得られた値は、オリジナルデータの偽造不可能な独自の指紋である。もしオリジナルデータが任意の態様で変えられれば、このように変更されたデータのハッシュも同様に異なるであろう。

【００８４】

関連セグメントのハッシングは、この発明に従って適切に権限を付与されたプログラムが後に手を加えられて、変更されたプログラムを結果としてもたらす可能性がないことを確実にする。セグメント２４にプログラムハッシュをストアすることによって、ハッシュは関連プログラムが権限が付与された後に変更されなかったことを保証するために後にチェックされ得る。セグメント２２において、特定のハッシングアルゴリズムを独自に識別する識別子がストアされる。

【００８５】

ＰＡＩはプログラム（またはオブジェクト）のタイプを識別するセグメント２６を任意に含むことが可能であり、たとえば関連プログラムが機械言語プログラム、特定のタイプの監視プログラム、などであることを示す。プログラムのタイプを識別するデータを与えることによって、このシステムはプログラムによって実行されるべき動作の性質に関する何らかの情報を備える。このような情報は、何か予期しない（そして恐らくはいたずら半分の）ことが発生しているという表示を与えることが可能である。ＰＡＩはまたそれが署名されたときのプログラムの名前（セグメント２８）および権限付与の日付（セグメント２９）を識別するフィールドを含み得る。

【００８６】

セクション３０は以下の一連の権限関連エントリのサイズを規定するセグメントである。このフィールドは残っているエントリが所望されるように区切られることを可能にする。

【００８７】

後に続く各権限エントリは、特定のエントリのサイズを規定するセグメントを含む（３２）。各エントリは同様にそれが関連する機能または資源３４のタイプを識別するセグメント３４を含む。たとえば、プログラムが他のプログラムにディジタル署名を求める権限を付与する権利を有し得るかどうかなどの、広範囲の機能が規定され得る。セグメント３６はセグメント３４で識別された包括的タイプ内にある特定的機能／資源を特定する。たとえば、特定的ユーザファイルはセグメント３６で指定されて、セグメント３４で特定された「ファイル」をより特定的に識別する。セグメント３４および３６は、所望されれば、単一セグメントに組合わされ得る。セグメント３６の「ワイルドカード」への参照は、たとえば、プログラムが予め定められた接頭辞、または接尾辞を有する任意のファイルにアクセスし得ることを示すことが意図される。たとえば、指定「Ａ＊」はプログラムは「Ａ」で始まるタグによって識別される任意のファイルにアクセス可能であることを示すであろう。同様に、セグメント３６はそのプログラムは「ＤＡＴＡ」で終わる任意のファイルにアクセスし得ることを示す、またはそのプログラムは指定された組のファイルにアクセスすることができないことを代替的に示し得る、エントリ＊ＤＡ

ＴＡを含み得る。このようなエントリはまたそのプログラムは任意のプログラムファイルを変えることができることを示し得る。セグメント３６はこのようにそのプログラムが何ができるかだけではなく、そのプログラムは何をする権限を付与されていないかを特定し得る。

【００８８】

図２に示されるセグメント３８は与えられた権限のレベルを特定する。たとえば、セグメント３８はそのプログラムは予め定められた組のファイルからの読出しを許可する権限のレベルを与えられているが、任意のこのようなファイルを変えるまたは消去する権限は否定されていることを特定し得る。

【００８９】

もしＰＡＩが異なったユーザに利用可能にされれば（所望の受信者に送信されるプログラムのために）、ＰＡＩにとってディジタル署名されることが望ましいかもしれない。単一の組織内においてさえ、オプションの権限署名を含むことは望ましいかもしれない。

【００９０】

権限署名は署名セグメント４０を含む。署名セグメント４０は署名者の証明（certificate)への参照、つまり署名者の証明を識別するための識別子を含む。この発明の好ましい実施例に従って、このようなディジタル証明は、ユーザのパブリックキーおよびユーザの名前を含む委任されたエンティティによって作成された（エンティティが満足するほどに正確である）ディジタルメッセージ、および恐らくはディジタルメッセージに署名する当事者によってユーザに与えられた権限の表現である。このような署名者の証明は、本発明者の米国特許第 4,868,877号および第 5,005,200号の教示を利用して好ましくは作成され、これらの特許はここにはっきりと引用により援用される。これらの特許に従って、証明は証明者によって与えられつつある権限および課せられている制限ならびにセーフガードを含むように構成され、たとえば、被証明者に対する財政上の制限、および被証明者に与えられる信用のレベルのような、証明者にとっての関心事を示す情報を含む。証明はまた、上に示された米国特許に具体的に教示されるように、被証明者に課せられる共同署名および副署名要求を特定し得る。

【００９１】

署名セグメント４０はまた署名日付、およびハンシュならびにパブリックキーの双方に対するアルゴリズム識別子を含み得る。セグメント４０は、たとえばプログラムに権限を付与する権限を与えて、予め定められたファイルを変更するために証明で指定された１つ以上の権限を特定する署名に対して呼出された権限を付加的に含む。付加的に、この署名はたとえば上述のセグメント２０ないし３８の全体を含む、権限付与仕様のハッシュを含む。

【００９２】

19

セグメント４０で識別された項目に関する署名者のプライベートキー動作の結果はセグメント４２にストアされる。これはＸ．５００に規定されるような標準的なディジタル署名であってもよいし、または本発明者の上述の米国特許の向上したディジタル署名教示に従うものであってもよい。付加的な（可能な第２ないし可能な第Ｎ番目の）署名（共同署名）は、セグメント４４、４６に示されたようにストアされ得る。任意に、権限署名はまたセグメント４８の上の署名に対するディジタル証明を含み得る。代替的に、このような証明は識別されたデータベースからアクセス可能である（が、署名が任意のそのようなデータベースにアクセスする必要性を伴わずに確証され得るように、関連署名のためのディジタル証明を含むことが好ましい）。セグメント４０ないし４８は上述の権限仕様に関連する権限封印を構成する。ここに参照されるディジタル証明／ディジタル署名技術に関するすべてのさらなる詳細は、Ｘ．５００のような標準的な技術、または上述の米国特許に関連するような向上した技術を含む、任意のディジタル署名技術で実行され得る。

【００９３】

この発明に従って、ＰＡＩは実行されるべきプログラムと関連する。図３ないし図６はプログラム権限情報をプログラムに関連付けるための４つの例証的なアプローチを示す。まず図３を参照して、この図はどのようにプログラム権限情報がアクセス制御下で、プログラムと関連して、ストアされるかを例証する。図３はプログラムのシステムのディレクトリの例証的な概略表現を示す。ディレクトリはプログラム１、２、…Ｎ（８０、８６…９２それぞれ）の各々の名前を表すデータを含む。

【００９４】

各プログラム名前識別子に関連するのは、それぞれインジケータ８２、８８、９４であり、関連プログラム、たとえばプログラム１のディスク９８上の場所を識別する（１０４）。付加的に、プログラム関連識別子の各々に関連するのは、それぞれインジケータ８４、９０、…９６であり、その関連プログラム権限情報、たとえばＰＡＩ　１の場所を識別する。プログラム権限情報ＰＡＩ１は別個のメモリデバイス１００にストアされているとして示されるが、それは所望されればその関連プログラムと同一のメモリ媒体にストアされてもよい。上に示したように、プログラムに関連するプログラム権限情報は、プログラム権限情報がユーザ自身によって発生され、（この場合は署名する必要はない）か、または第三者によって発生され、この場合はＰＡＩはしばしば署名されなければならないかに依存して、ディジタル署名されてもよいし署名されなくてもよい。

【００９５】

図４はＰＡＩをプログラムに関連づける他のアプローチを示す。このアプローチにおいて、プログラム権限情

20

報１１０はプログラム１１２にはめ込まれる。図３に関連して上に説明したように、権限付与情報はＰＡＩの源に依存して、任意にディジタル署名されてもよい。

【００９６】

図５は、ＰＡＩデータ構造がこの発明の一実施例に従うプログラムと関連する重要なアプリケーションを示す。図５は安全な交換可能な「オブジェクト」のための例示的なデータ構造を示す。このデータ構造は委託された権限によって署名され得る。このようなデータ構造の署名により、オブジェクトはユーザからユーザへ安全に送信されることが可能になる。図３、図４、図５および図６に示されるデータ構造は一般的なフォーマットで説明されているが、１９９２年４月６日に出願され、「移動プログラムを作成し支持しかつ処理するための方法および装置（Method and Apparatus for Creating, Supporting and Processing a Travelling Program）」（米国連続番号０７／８６３，５５２、Ａｔｔｙ．Ｄｋｔ．２６４－３０）と題された、本発明者の同時係属中の出願で説明されたような構造であってもよく、この出願は引用によりここに明示的に援用される。

【００９７】

データ構造は、ほんの一例として、たとえば買注文関連オブジェクトまたは任意の他のタイプの電子ディジタルオブジェクトに続くタイプのオブジェクトを規定し得るヘッダセグメント１１４を含む。プログラム権限情報は、以下により詳細に説明される態様で、オブジェクトの単数または複数のプログラムのための権限を特定するセグメント１１６にはめ込まれる。

【００９８】

データ構造はオブジェクトプログラムセグメント１１８を含み、それはたとえば、関連する買注文がプログラムユーザによって対話的に完了される変数フィールドのためのブランクを残すようにディスプレイされる態様を制御し得る。オブジェクトプログラムはそのようなデータをストアし、出願人の上述の同時係属出願に詳細に説明される態様でそれ自体のコピーを添付データとともに送る。図５に示されるように、このプログラムは数個の論理セグメントに分割されて、オブジェクトの異なった用途を収容し得る。たとえば、このプログラムはディジタル買注文を作った人に、後続の受信者にディスプレイするのとは異なったディスプレイを示し得る。プログラムがプログラムによって指定された受信者によって受信された場合、その受信者は送信されたプログラムの写しを呼出して、たとえば受信者の必要に合わせて作られた買注文のディスプレイを制御する。受信者はすべての受信されたデータを確証し、新しいデータを加えることが可能であり、プログラムはそれ自体を受信者の電子メールシステムによって、たとえば購入された品物を実際に出荷するユーザに送ることが可能である。

【００９９】

図５に示されたデータ構造は付加的にオブジェクトに関連するデータセグメント１２０を含み、それは好ましくは上述の特許出願に説明されるような「変数」セグメントおよびデータファイルセグメントを含む。データセグメント１２０はオブジェクトの各バージョンまたはインスタンスに関連するデータが別個にストアされ、別個にアクセス可能であるように区切られてもよい、なぜなら異なったユーザは図５に示されるデータ構造に対して異なった用途を有するかもしれないからである。したがって、データはそれが各ユーザからどのように集められるかに依存して変化することになる。しかしながら、プログラム１１８は好ましくは各ユーザに対してそのままである。委託された権限はプログラム権限情報（ＰＡＩ）とともにプログラムに署名する、なぜならプログラムの各実行に応答して入力されるデータよりはむしろ、プログラムそれ自体が権限付与される必要があるからである（データは各実行経路の間変化することが可能であるからであり、かつまた正確なディジタル署名が適切に入力データ上で集められることを確実にすることはプログラムの責任であるからである）。

【０１００】

図６は多くのユーザが同一のプログラム（イメージ）にアクセスする状況を例証し、各々はそれに関連し、ユーザに所属する特定的ファイルに維持される自分自身の（おそらくは別個の）プログラム権限情報１２９を有する。図６はシステムプログラムディレクトリ１３１を示し、それはプログラム名前に関連するインジケータによって、プログラムＸのディスク１３２上の場所を識別する。この場合、プログラムＸがユーザによって呼出された場合はいつでも、システムはユーザがそのプログラムに関連し得るプライベートなＰＡＩ仕様（たとえば１３３、１３５、１３７）を有するかどうかを決定するためにチェックする。このように、異なったユーザは自分自身の必要性および信用の知覚に従ってプログラムを制限し得る。これはたとえば大きな固有の権限を有するユーザ、または非常に重要な情報へのアクセスを与えられたユーザが、ありきたりの目的のための「平凡な」プログラムをしばしば実行しなければならない場合に有用であり得る。この場合、そのような重要なユーザにとって、いくつかの（または多くの、またはすべての）「平凡な」プログラムのまわりに「セーフティボックス」を規定して、その結果そのようなプログラムが自分自身の特に重要なデータに影響を及ぼし得る「トロイの木馬」または他の欠点を不注意に含まないようにすることが分別のあることかもしれない。

【０１０１】

したがって、このようなユーザは一般的なＰＡＩ「関連付け」を規定し、その結果保護しているＰＡＩは、重要なデータを処理する選ばれて委託されたいくつかのプログラム（select trusted few programs)をおそらく除

いて、すべてのプログラムに自動的に関連し得る。

【０１０２】

この発明はＰＡＩ情報が任意の適切な態様で関連づけられることを許容し、その結果原則的にユーザはおそらくはより総括的なＰＡＩ、またはこのプログラムの製造者によって署名されかつ供給されたＰＡＩとともに組合わされる１つ以上のレベルのＰＡＩを規定することが可能である。

【０１０３】

この発明はプログラムとそのＰＡＩとの間の関連付けが、もし必要であれば、１つのプログラムが複数のＰＡＩと関連することが可能であるように、または逆に１つのＰＡＩが複数のプログラムに適用されることが可能であるように、またはこれらのアプローチの何らかの組合わせが可能であるように非常に一般的に構成され得ることを熟慮する。したがって、単純にするために、本明細書では単一のＰＡＩを単一のプログラムと関連して一般に論じているが、これはいかなる意味においても制限であると考えられてはならないことが理解されなければならない。

【０１０４】

図７は特に不明の信用性のプログラムを実行する場合に、どのようにユーザがプログラム権限情報の使用によって利益を得るかを例示するフローチャートである。ブロック１２１に示されるように、ユーザは自分がプログラムの作成者について何も知らない興味あるプログラムを実行したいという望みを持つかもしれない。このように、そのプログラムは不明の信用性を有し、たとえば電子掲示板を経てアクセスされたものかもしれないし、テレコミュニケーションチャンネルまたはディスケットを経てユーザの端末に到着したものかもしれない。単なるゲームであると称するこのようなプログラムは、それがウィルスに感染しているかもしれないという重要な危険をはらんでいる。

【０１０５】

ブロック１２２で示されるように、ユーザはそのプログラムを重要でないまたは消耗ファイルのみに制限するプログラム権限情報を規定することによって保護され得る。所望されれば、ユーザはとにかく任意のファイルを変更することからこのようなプログラムを制限することが可能である。たとえば、ユーザはプログラムにディスプレイスクリーンにイメージをディスプレイし、ゲームをすることに関連する機能を実行することのみを許可し得る。代替的に、もしプログラムが単一のワークファイルを有することがわかれば、ＰＡＩデータはそのような単一ファイルの使用のみを許可することが可能である。単一ワークファイルのみにアクセスを制限することによって、不明の信用性のプログラムは他のユーザのプログラムにウィルスを導入することができないし、または他の態様ではシステムプログラム誤動作を開始することが

できない。このように、この発明に従って、ユーザは、システムプログラムによって、プログラムの任意の特権機能を使用する能力をたとえば完全に排除するようなプログラムによる危険にユーザのシステムがどれくらいさらされるかを決定する。ユーザはそれからたとえばオペレータを促すメニュー駆動型システムによって、ＰＡＩをそのシステムに基づいて実行されるべきすべてのプログラムに関連づける（またはこのようなＰＡＩまたはＰＡＩの欠如を予め定められた省略時（default)メカニズムによって関連づける）。システムユーティリティプログラムは、図９ないし図１３と関連して以下に詳細に説明される態様で、プログラム権限情報を作成するために好ましくは使用される。

【０１０６】

ＰＡＩが割当てられた後、そのシステムが関連するプログラムを実行するときはいつでも、システムソフトウェアは（以下に説明される態様において）プログラムがＰＡＩと一貫する態様で安全に実行していることを確実にする。このように、プログラムは「セーフティボックス」に有効に置かれたことになる（１２４）。

【０１０７】

図１に戻って、不明の信用のプログラムはコミュニケーションチャンネル１２によって、または端末Ａにロードされたフロッピィディスクからシステムに導入され得る。このプログラムはたとえばユーザのプログラムディスクメモリ７に初めストアされ得る。その後、キーボード４上のユーザは（図７のブロック１２２に関して）上で識別されたシステムのプログラムとの対話を介して、そのプログラムがユーザのシステムに基づいて安全に実行できるように、またはおそらくはＰＡＩがプログラムとともに到着し、その場合にはおそらく署名されるように、（図３ないし図６に示されたような態様で）、プログラムにプログラム権限情報を関連づける。

【０１０８】

図８はこの発明の例証的な実施例に従うプログラムコントロールブロック（ＰＣＢ）データ構造の例示である。プログラムコントロールブロック１４０はシステムモニタによって使用されて関連するプログラムの実行を制御するデータ構造である。

【０１０９】

プログラムコントロールブロック１４０には、関連するプログラムがプログラムがその割当てられた権限に従って機能を実行し、資源にアクセスすることを確実にするように実行されているときに、ＰＡＩが容易に参照され得るように、プログラム権限情報がロードされる。実行されるべきプログラムと関連するプログラムコントロールブロックは、プログラムによって変更することができない記憶エリアに置かれる。

【０１１０】

図８に示されるように、親プログラム（そのＰＣＢは

１８０で識別される）はプログラム（ＰＣＢ１７０を有する）を呼出し、それはひいては図８に詳細に示されるプログラム１４０を呼出す。各新しいＰＣＢは「以前の」または呼出しているプログラムコントロールブロックを指す１５０のようなフィールドを含む。フィールドはまた「次の」プログラムコントロールブロックファイルを識別するために使用され得る。

【０１１１】

呼出されたプログラムが実行を終えた場合、システムはその関連するＰＣＢを実行されたスタックの一番上から取除き、関連するプログラムを記憶から取除き、関連する権限付与情報を取除き、スタックのその真下のプログラムコントロールブロックにアクセスする。他のプログラムが呼出された場合、スタックの一番上に置かれた新しいＰＣＢが作られるように逆のプロセスが発生し、それはフィールド１５０に示されるように以前のＰＣＢを再び指す。

【０１１２】

プログラムコントロールブロックはまた、図８に示されるメモリセグメント１５３によってたとえば示されるように、関連するプログラムがロードされている記憶の場所に対するポインタであるフィールド１５２を含む。付加的に、プログラムのサイズはフィールド１５４で示される（それはこのようにしてプログラムが実行を終了した場合に解放される記憶の量を示す）。

【０１１３】

プログラムコントロールブロックのフィールド１５６は、１つ以上のＰＡＩの記憶（１５７）の場所を識別する（それは関連するプログラムによって変えることができない記憶のエリアに置かれる）。フィールド１５６によって指されたＰＡＩは好ましくは上述の図２に示された態様で構成される。

【０１１４】

フィールド１５８は関連するプログラムのためのエントリアドレスを識別する。もしプログラムがその実行中に他のプログラムを呼出せば、フィールド１５８は、呼出されたプログラムがその実行を完了した後、プログラム実行が再開されるであろうアドレスをストアするために使用される。

【０１１５】

プログラムコントロールブロックはまた、たとえばプログラム状態ワード（ＰＳＷ）スタック情報などのような状態情報をストアするための１組の場所（１６０）を含む。プログラムコントロールブロックは、付加的に、もしエラーがプログラムの実行中に発生すれば、エラーまたは終結メッセージに関連する情報をストアするためのフィールド１６２を含む。このようなフィールドは、たとえば、なぜプログラムが不成功に終結したかを識別するための呼出しプログラムに利用可能である。フィールド１６２はプログラムが成功のうちに終結したという

表示をストアすることが可能である。

【０１１６】

プログラムコントロールブロック１４０は、プログラムが終わった場合に（１６４）漂遊（stray)資源が解放され得るように維持される様々なポインタを付加的に含む。このようなポインタはたとえばプログラマーが解放するのを忘れた資源の解放を許容するために有用である。

【０１１７】

図９ないし図１２はプログラム権限情報を確立するためのユーティリティプログラムの動作の例証的なシーケンスを例示するフローチャートである。このようなユーティリティプログラムはユーザ、つまりエンドユーザ、エンドユーザの主体または製造者でさえ促して、ユーザのシステムによって実行されるべきプログラムに関連する権限の範囲を規定する。

【０１１８】

図９に示されるように、ＰＡＩを確立するためにユーティリティプログラムを入力した後（２００）、ユーザはそれに対してＰＡＩが確立されるべきプログラムの名前を供給するように促される（２０２）。その後、ユーザはＰＡＩは署名されるべきか署名されるべきでないかを決定するように促される。ＰＡＩは、もしそれがユーザ自身の使用および保護のためのものであれば、またはもしこのＰＡＩが満足なアクセスコントロールの下でストアされ得るのであれば、必ずしも署名される必要はない。ブロック２０４のユーザの入力に依存して、ユーザが署名したいのかまたは署名したくないのかについての決定が行なわれる（２０６）。もしユーザが署名したいのであれば、ブロック２０８に示されるように、ユーザの証明が検索され、後のテスティングのためにフラグが設定され署名動作が実行されていることを示す。ユーザの証明は従来のディジタル証明であってもよいし、本発明者の米国特許第 4,868,877号および第 5,005,200号に従う権限の委譲を与える向上されたディジタル証明であってもよい。

【０１１９】

ブロック２１０で示されるように、ユーザはそれからどの権限がプログラムに割当てられるべきか指定するように促される。後に続く権限（そしてそれらが示される順序）は例示の目的のみのために与えられ、かつこの発明に従って割当てられ得るすべての可能な権限の完全なリストであることは意図されないことが理解されなければならない。

【０１２０】

図９に例示されるように、ファイルアクセス権限が呼出されるべきであるかどうかを決定するためにチェックが行なわれる（２１２）。ファイルアクセス権限（および以下に参照される他の権限の各々）の選択を与えるために、メニューがユーザに表示されてもよい。ファイル

アクセス権限は任意の組のファイルのファイルエレメントもしくはフィールド、任意の組のデータもしくはデータエレメント、または任意の組のファイルなどに関する権限を示すために使用され得ることが理解されなければならない。もしユーザがファイルアクセス権限を選択すれば、ユーザはファイル名またはファイルステムまたは「ワイルドカード」ファイル名パターンを特定するように促されるであろう（２１４）。上に説明されたように、たとえば、ワイルドカードファイル名パターンはフォームＤＡＴＡ＊から選択されることが可能であり、その結果プログラムは接頭辞「ＤＡＴＡ」で始まる任意のファイル名にアクセスする権限を与えられる。

【０１２１】

その後、ユーザはファイルアクセスのタイプを特定するように促される（２１６）。この点に関して、ユーザはプログラムの権限を、ファイルから読出す、情報をファイルに挿入する、ファイルの情報を更新する、ファイルから情報を消去する、ファイルを消去する、ファイルを転送するなどだけの中から、１つ以上に制限することを特定し得る。もしファイルアクセスまたは図９ないし図１１で以下に示される他の権限が選択されれば、この選択の表示がストアされ、ルーチンは以下に説明される図１２および図１３のブロック２７４に分岐する。

【０１２２】

もしユーザがファイルアクセスを選択しなければ、これはこのプログラムに他のプログラムを呼出す権限を付与するための要求であるかどうかを決定するためにチェックが行なわれる（２１８）。もしそうであれば、プログラムがそれに基づいて呼出され得る、もしあれば、何の制限または資格が確立されるべきであるかを確認するために決定が行なわれる（２２１）。そのような資格が規定され組合わされ得る多くの方法がある。たとえば、１つの特定のプログラム名のみが呼出されることが許容されることであってもよいし、またはおそらくある（「ワイルドカード」）パターンに一致する名前を有するプログラムのみが呼出されてもよい。おそらくその基準はライブラリ、または組のライブラリの仕様を含み、そこには許可されるプログラムが存在し得る。

【０１２３】

このプログラムによって呼出されるのに相応しいプログラムを資格付ける他の方法は、呼出されたプログラムが呼出しているプログラムほど大きな権限を有してはならないことを特定することである。代替的に、権限および必要性に依存して（およびどのようにシステムが呼出しているおよび呼出されたプログラムの権限を組合わせるように選択するかに依存して）、呼出されたプログラムが呼出しているプログラム以上の権限を有することを要求することが適切であり得る。実際、この「呼出し権限」資格の一部として、それによって権限が呼出されたプログラムと組合わされることが可能な（たとえば呼出

されたプログラムの自然の権限を使用することによって、呼出されたものおよび呼出すものの最も制限的な権限を使用することによって、など）方法を特定することさえ適切であるかもしれない。

【０１２４】

ここで使用されるように、特定された権限の資格または制約または制限または許可へのいずれの参照も、適切な基準の任意の収集に基づいて設定された全体の規則仕様を含むことが意図される。「規則」「組の」、「資格」などの言葉はその最も一般的な意味で使用され、それによって仕様は任意のタイプの規則または規則の複合組によって決定されることが可能であり、それはたとえば、制限なしに、直接仕様による、間接仕様による、排他による、リストによる、「ワイルドカード」規則による、または任意の適切な属性、方法または基準によってエレメントを区別する他の任意の方法によることを含む、任意の属性によってエレメントを区別することが可能である。そのような区別は単一のエレメントのみを含む、すべてのエレメントを除外する、またはすべてのエレメントを含む仕様を包含することが意図される。ＰＡＩは全体または一部において、任意の数の隣接するまたは隣接しないデータのセグメントからなり得る。適切な文脈において、その文脈のために公式化される予め定められた規則があってもよく、それは任意の明示的な資格がない場合に推定される。

【０１２５】

「示す」、「～を指す」、「のアドレス」などの言葉は、たとえば直接仕様、任意のタイプのポインタ、参照、関連、ハッシュ、結合値共通識別子、などを、制限なく、含む適切な関連の任意のタイプを伝えることが一般に意図され、それは任意のレベルの間接性（indirection)を含んでもよく、明示性であってもよく、または任意の明示の関連がないところでも文脈に適切であれば暗示であってもよい。

【０１２６】

「制限」という言葉は制限の一般的な概念を示すことが意図され、しばしば通常の能力に対する「制約」と共通の意味で使用されるが、制限が通常の能力を超えて規定される状況を反映することもまた意図される。

【０１２７】

この発明は、プログラムの能力を通常ユーザに許された資源にアクセスすることに制限する機能を規定することに主に中心を置くが、適切な環境において、ユーザに通常許容された能力を超えるものに拡張するためにも使用され得る。このように、たとえば、そのＰＡＩがスーパバイザによって認められた権限によって署名されるプログラムは、拡張された機能を実行することが許容される。

【０１２８】

いくつかの例証的な規則がＰＡＩがどのように確証さ

れるべきかに関して与えられたが、特定の実施例は広く変わり得る。示されたように、いくつかの場合、ＰＡＩはまったく署名される必要はなく、それはたとえばユーザ自身がＰＡＩを規定する場合、または信用された管理者がＰＡＩを信用されたアクセス制御された記憶にストアする場合などである。ＰＡＩが署名された場合、署名確証が、たとえば本発明者の他の特許、米国特許第 4,868,877号および第 5,005,200号に従って行なわれる任意の数の方法がある。ユーザは最終的なパブリックキー、またはその署名をユーザが信用する証明を規定する以前にストアされた情報を有するようである。

【０１２９】

図９に戻って、もしユーザがプログラム呼出し許可を選択しなければ、これはこのプログラムが呼出され得る状況を特定するための要求であるかどうかを決定するためにチェックが行なわれる（２２０）。もしそうであれば、そのような権限の制限または資格を確認するための決定が行なわれる（２２３）。１つのそのような仕様は、プログラムはユーザによって直接呼出されなければならない（かつおそらくはこれは任意の仕様の代わりに暗黙値であろう）ことであり、おそらくはこのプログラムは特定のリスト、または上述の「呼出し権限」に類似の特定ライブラリからの名前でプログラムによって呼出されるだけである。おそらくプログラムはより大きな権限を有する、またはより小さな権限を有するプログラムによって呼出されるだけである。どの規則が適切であるかは、基礎になるシステムが他のプログラムによって呼出されたプログラムのためのＰＡＩ権限をどのように組合わせるかに関連し得る。この資格の他の局面は、このプログラムの権限がどのように呼出しているプログラムの権限と組合わされ得るか、たとえばこのプログラムの有効な権限は呼出しているものによって制限されるかどうかを特定することであり得る。他の多くの可能性もまた利用可能であり、権限の各タイプごとにおそらく異なる。

【０１３０】

図１０に移って、もしブロック２２０で識別された権限が選択されなかったならば、プログラムが電子郵便を生成することを許容されるべきか否かを決定するためのチェックが行なわれる（２２２）。もしそうであれば電子郵便を生成するこの能力が資格付けされるべきか、たとえば或る個人に限定されるべきか否かのチェックが行なわれる。もしそうであれば、このようなさらなる資格がユーザによって特定される（２２４）。

【０１３１】

もしブロック２２２で識別された権限が選択されなければ、ユーザはプログラムが他のユーザへデータを伝送することを許容されるべきか否かについて問われる（２２６）。もしそうであれば、ブロック２２４の上述の処理が行なわれ、この権限に対するいかなる資格も決定す

る。

【０１３２】

もしブロック２２６で識別された権限が選択されなければ、ブロック２２８に示されるように、プログラムが「文書解放（document release）」動作を行なうことを許容されるか否かを決定するためのチェックが行なわれる。もしそうであれば、たとえば権限が適用される文書のクラス（たとえば極秘（top secret）、機密（secret）、機密扱い（sensitive）、など）をユーザから決定することによってこの権限に対する資格が選択され、記憶されてもよい。代替的に、解放されるべき文書はセキュリティの観点から「解放」を要求しなくてもよいが、むしろ文書の技術的解放に関連してもよい。いずれにおいても、どのような選択された資格も記録される。

【０１３３】

もしブロック２２８で識別された権限が選択されなければ、プログラムが機械語プログラムを実行することが許容されるべきかを決定するためのチェックが行なわれる（２３２）。この権限は或るルーチンが機械語プログラムとして不適当に実行するか、または実行されることを防止するのに有用であろう。ユーザは任意の適当な資格を特定するように促されてもよい（２３３）。もしブロック２３２で識別された権限が選択されなければ、プログラムが任意の特別なメモリアクセス特権、たとえば或るオペレーティングシステムプログラムのために予約された記憶域へのアクセスが与えられるべきであるか否かを決定するチェックが行なわれる（２３４）。もしそうであれば、ユーザはこのようなアクセス特権へのいかなる資格も適当なものとして特定することが促されるであろう。

【０１３４】

もしブロック２３４で識別された権限が選択されなければ、プログラムがユーザへ情報を表示する権限を有すべきか否かを決定するチェックが行なわれる（２３８）。この点で、或るプログラムが或る計算を行なう目的のみを意図されてもよい。このようなプログラムはいかなるユーザ対話も存在してはならないように設計され得る。もしこのようなプログラムが許可なく変更されたとすれば、ユーザへ誤ったメッセージを作成する命令が挿入されているかもしれず、それがセキュリティ侵害を引き起こすかもしれない。たとえば、システム障害があるということ、および動作を再開するためにユーザが自分の秘密のパスワードを入れることが必要であるということをスクリーンがユーザへ表示し得る。このようなプログラムは当事者へパスワードを自動的に伝送し得、するとその当事者はパスワードおよびそのような画面上に入れられた他のいかなる情報へもアクセスを有するであろう。

【０１３５】

ブロック２４０に示されるように、もしプログラムが

ユーザへ情報を表示する権限を与えられれば、この権限は、たとえば特別なウィンドウ内に、または特別なコンソール上のみに表示を許可するだけで制限されてもよい。

【０１３６】

もしブロック２３８で識別された権限が選択されなければ、図１１、ブロック２４２に示されるように、プログラムがユーザからの入力を請求する権限を有するべきか否かについてのチェックが行なわれる。もしそうであれば、この権限は、たとえば特別なウィンドウまたは端末からの請求により可能性のある制限の特定によって、資格付けされてもよい（２４４）。

【０１３７】

もしブロック２４２で識別された権限が選択されなければ、プログラムがディジタル署名を請求する権限を有するべきか否かに関するチェックが行なわれる（２４６）。この点で、１組の情報を表示することによっていたずら半分のプログラムがユーザを引っかけるかもしれないが、それによって実際のディジタル署名が全く異なる組のディジタル材料へ与えられる。それゆえ、ディジタル署名動作を請求する、および／または行なうＰＡＩ権限を要求することによって、権限を付与されないプログラムは権限を付与されたプログラムの外部属性を真似るが、ユーザのディジタル署名能力を詐欺まがいの材料へ内部的に与えることを防止される。

【０１３８】

もしプログラムがディジタル署名を請求することを許可されれば、ブロック２４８に示されるようにこの権限に制限が加えられてもよい。したがって、プログラムは制限された範囲、値、権限または他の特性を有する材料にディジタル署名を行なうことのみが許容されるであろう。

【０１３９】

もしブロック２４６で識別された権限が選択されなければ、プログラムがロボット装置、または特定のコンピュータ機器もしくはコンピュータ関連装置へ向ける権限を有するか否かを決定するチェックが行なわれる。もしこのような権限が選択されれば、このような機器に及ぼす制御の詳細および範囲を特定することによってこのような権限に資格が与えられてもよい（２５２）。

【０１４０】

もしブロック２５０で識別された権限が選択されなければ、アクセスが一般にセキュリティクラスによって制限されるべきか否かを決定するチェックが行なわれる（２５４）。したがって、或る資源、ファイルなどが機密、機密扱いなどのような特定のセキュリティクラスと関連され得る。もしこのような権限がプログラムと関連されるべきであれば、特定のセキュリティレベルの指定を含む制限が同様に特定されてもよい（２５６）。

【０１４１】

もしブロック２５４で識別された権限が選択されなければ、他のコンピュータ機能、または資源が制御されるべきであるか否かについてチェックが行なわれる（２５８）。もしそうであれば、ユーザはこのような他のコンピュータ機能、または資源についての詳細を特定することが促される（２６０）。

【０１４２】

もしブロック２５８で識別された権限が選択されなければ、図１２に示されるように、ユーザが権限の特定を終了したか否かを決定するチェックが行なわれる（２６２）。もしユーザが権限の特定を終了していなければ、権限選択のアレイがこの点で消耗されているために、不明の特定された権限を特定することをユーザが試みていることを示すメッセージが発行される（２６４）。ルーチンは図９へルーチン分岐して戻り、エントリポイントＧでブロック２１０における処理を再開する。

【０１４３】

ブロック２６２に定められるように、もしユーザが権限の特定を終了していれば、前に規定された権限のすべてが収集され、図２に示されるＰＡＩ構造がディジタル署名関連のエントリを除いて完了する。

【０１４４】

ブロック２６８で、ＰＡＩがディジタル署名されるべきか否かを決定するチェックが行なわれる。もしそうであれば、ブロック２７０に示されるように、適当なディジタル署名動作がＰＡＩ上で行なわれる。ディジタル署名は本発明者の米国特許第4,868,877 号および5,005,200 号における教示に従ってか、または所望されるような従来のディジタル署名および証明技術を使用して行なわれてもよい。その後、ＰＡＩは、たとえば図３ないし図６に説明されるアプローチの１つを使用して記憶され、それによってそのプログラムと関連付けられ（２７２）、その後ルーチンが退出する。

【０１４５】

図１３に移って、エントリポイントＦで、ブロック２１２ないし２５８に関して説明された権限の各々が選択され、選択の指示が記録された後、ルーチンは分岐してブロック２７４へ進み、権限の特定がディジタル署名しているか否かを決定する。もし権限がディジタル署名されていなければ、新たに規定された権限が関連のプログラムのための権限情報へ加えられ（２８０）、ルーチンは図９のエントリポイントＧでブロック２１０へ分岐して戻る。

【０１４６】

もし権限がディジタル署名されるべきであれば、向上した証明（権限を有する）が本発明者の米国特許第4,868,877 号および5,005,200 号に従って使用されているか否かについてのチェックが行なわれる（２７６）。もしそうでなければ、ルーチンは前述のようなブロック２８０へ分岐する。

【０１４７】

もし向上したディジタル署名が使用されていれば、前述の特許に説明されるようなユーザの向上した権限証明がこの特定のプログラムの権限特定を割当てることを許可するか否かを決定するチェックが行なわれる。もし向上した権限証明がこのような権限の割当てを許可すれば、ブロック２８０の前述の処理が行なわれる。もしそうでなければ、ブロック２８２に示されるように、「あなたの証明はこのレベルのプログラム権限の割当てを許可されていません。」というメッセージがユーザへ発行される。ルーチンは図９およびブロック２１０の処理のためのエントリポイントＧへ分岐して戻る。

【０１４８】

図１４および図１５は、そのプログラム権限情報に従って実行されているプログラムの処理を制御するためのスーパバイザプログラムの動作のシーケンスを示す。図１４に示されるプログラム「Ｘ」およびそのプログラム権限情報の処理は、コンピュータがスーパバイザルーチンを実行している間に開始される。図１４の３００で示されるように、呼出プログラムは実行のためにプログラムＸを呼出す。その後、プログラム制御ブロックがプログラムＸのために作成される。作成されたプログラム制御ブロックは、プログラムが呼出されることを許可されることが決定され、かつ確証がうまく完了されるまで、実行スタックの先頭に加えられないであろう。したがって、もしプログラムがセキュリティチェックを失敗すると、それはプログラム実行鎖に置かれないであろう。「試験的」プログラム制御ブロックを作成することに加えて、呼出されたプログラムはブロック３０２の処理中に適当なプログラムディレクトリを介して位置決めされるであろう。

【０１４９】

その後、ブロック３０４で、ＰＡＩが前述のいわゆる「セーフティボックス」内にプログラムＸを置くようにプログラムＸとまだ関連されているか否かを決定するチェックが行なわれる。このＰＡＩは前述のようなその特定の応用によって署名されても、されなくてもよい。

【０１５０】

もしいかなるＰＡＩもプログラムとまだ関連されていなければ、プログラムが製造者からの関連の署名された「系統（pedigree）」を有するか否かを決定するチェックが行なわれる（３０６）。したがって、もし周知のプログラム製造者がパブリックキー、またはディジタル証明でプログラムに署名しているならば、所望ならこのようなプログラムが、製造者がどれだけ信用しているかによって所望のどのような権限レベルを割当てられてもよく、システムはこのようなプログラムの実行を許可してもよい。製造者からのこのようなディジタル署名は、プログラムが製造者によって生成されたときと全く同じであるか否かを決定されることができるので、関連のプロ

グラムがウィルスによって感染されていないということを確証するために使用され得る。

【０１５１】

もしブロック３０６のチェックが、ブロック３０８で製造者からのディジタル署名があるということを示せば、ユーザによって前に確立されている、（かつユーザが前に信用を確立した製造者によって署名されている）信用基準があるとすれば、ディジタル署名を確証し、適切である証明および権限チェックのいかなるものも行なうことによって、製造者の「系統」が確証されるであろう。権限を委任するディジタル署名を行なうための機構は、本発明者の米国特許第 4,868,877号および 5,005,200号に詳細に特定され、これらの特許は引用によってここに明確に援用されている。

【０１５２】

ブロック３０８の確証動作の結果によって、ブロック３２０で、製造者の系統が認容可能であるか否かについての決定が行なわれる。もし製造者の系統が認容可能でなければ、ルーチンはブロック３２４へ分岐し、そこでプログラムの実行が以下に説明されるであろうように抑制される。

【０１５３】

もし製造者の系統が認容可能であれば、ルーチンはブロック３２６へ分岐し、そこで記憶域がプログラムについて割当てられ、プログラムは以下に詳細に説明される態様でロードされる。

【０１５４】

ブロック３１０で示されるように、もしＰＡＩがプログラムＸに関連していると決定されれば、ＰＡＩが署名されるか否かを決定するチェックが行なわれる。もしＰＡＩが署名されれば、ブロック３１６で示されるように、署名が確証される。現在好ましい実施例において、署名が証明階層を通して確証される。署名が有効であるか、それらが呼出人によって信用されているか、およびプログラムによって委任された権限が署名者によって委任されていることを許可されるかを決定するための好ましい方法論が本発明者の米国特許第 4,868,877号および 5,005,200号に教示される。これらの特許に示されるように、信用レベルはどの高レベルのパブリックキー、および／または超証明子（metacertifier)がユーザによって信用されるように特定されているかによって決定されてもよい。代替的により慣習的なディジタル署名技術が使用されてもよい。

【０１５５】

ブロック３１６の処理によって、ブロック３２２で署名が有効であり、権限が付与され、かつ信用されているか否かの決定が行なわれる。もし署名が有効であると決定されなければ、ルーチンはブロック３２４へ分岐し、そこでプログラムＸの実行が抑制される。

【０１５６】

もしブロック３１０のチェックが、ＰＡＩが署名されていないということを表わせば、３１２で特定のシステム、またはアプリケーションが、ＰＡＩが署名されることを要求するか否かについてのさらなるチェックが決定される（３１２）。もし、たとえばユーザ生成されたプログラムがユーザ自身の使用のために実行されていれば、プログラムは分配されておらず、かつユーザは自分が行なったことを信用しているので、署名は必要でないであろう。もしブロック３１２でディジタル署名が必要でなかったと決定されれば、ブロック３１８は署名されないＰＡＩを受取り、かつこれを使用し、記憶域が割当てられ、プログラムＸがロードされるであろう（３２６）。

【０１５７】

もしブロック３１２でディジタル署名が必要であると決定されれば、ブロック３１４で、明示ＰＡＩまたは署名されないＰＡＩを有さないプログラムのための「最小の」権限省略値をシステムが有するか否かについてのチェックが行なわれる。したがって、たとえばシステムは、いかなる永続ファイルも変更することを試みない限り、最小の権限省略値下でプログラムが実行することを許可してもよい。もし最小の権限省略値がなければ、プログラムの実行は抑制される（３２４）。プログラム実行の抑制過程において、エラーコード、またはメッセージが呼出プログラムへ戻されるであろう。たとえば、「プログラムＸは有効な署名された権限を有さない」というメッセージが呼出プログラムへ表示されてもよい。ルーチンはブロック４１０へ分岐し、そのブロックはさらに後に説明されるであろうように実行を実際に抑制するように作動する。

【０１５８】

もしブロック３２２および３１６の処理が署名が有効であることを明らかにすれば、ブロック３２６の処理が行なわれる。まず、記憶域がプログラムについて割当てられる。プログラムはメモリ内にロードされてもされなくてもよく、このメモリはスーパバイザのみがコンピュータシステムおよびプログラムの性質に組込まれた制約によって変えることを許容される。もしプログラムがそれ自体を変更すれば、それはスーパバイザのみが変えることを許容されるメモリ内にロードされることができない。

【０１５９】

その後、プログラムＸのプログラム権限付与情報が、もしあるならば呼出プログラムのＰＣＢと関連のＰＡＩと適当に組合わされる。多数のＰＡＩのものを含み得る組合わされたＰＡＩはプログラムによって一般に変更され得ない記憶域内に記憶され、ＰＡＩのアドレスは図８のフィールド１５６に示されるようにプロセス制御ブロック（ＰＣＢ）内に記憶される。したがって、プログラムＸはもし呼出プログラムによって呼出されれば、それ

自身の制約のすべてを受けるとともに、呼出プログラムの制約とある点で組合わされており、その集合制約はプログラムＸのＰＡＩに具体化される。この態様において、呼出プログラムは単に別のプログラムを呼出すことによってその割当てられた境界を超えることが許可されない。プログラムのＰＡＩが、プログラム自体の固有の性質、および現在の環境に適用可能である方策によって、それを呼出すプログラムのＰＡＩと組合わされ得る、多くの代替方法がある。組合わせ方法でさえそれ自体、呼出す、または呼出されたプログラムのいずれか、または両方のＰＡＩ権限、または資格付けるものの１つであり得る。

【０１６０】

たとえば、呼出されたプログラムをその「通常の」ＰＡＩ権限の小さい方およびその呼出プログラムのそれに制限し、呼出プログラムが呼出されたプログラムの大きい方の権限をいたずら半分に誤用してそれ自身の制限を巧みに回避できないことを保証することが穏当である。

【０１６１】

他方、それら自身の処置を注意深く確証する呼出されたプログラムでは、呼出されたプログラムにそれを呼出すプログラムより大きい固有の権限を許容することが可能であり得、このように高感度の資源がより広い使用を、信用されたサブプログラムを通してこのような使用を取り次ぐことによって利用可能にされ得る。このような組合わせの可能性は基本的制御システムの設計者によってだけではなく各プログラムへの権限の割当てを行なう者によっても注意深く検討されねばならない。その後、プログラムはロードされ、プログラムのハッシュがプログラムのＰＡＩに特定されるアルゴリズムに基づき計算される。

【０１６２】

プログラム３１４に戻って、もしシステムが最小の権限省略値を有すると決定されれば、ブロック３２８に示されるように、最小の省略値権限が使用される。このような最小の省略値権限はもしあれば呼出プログラムのＰＡＩと適当に組合わされ、ブロック３２６に関連して上に説明されたように新しいＰＣＢ内に挿入される。ＰＡＩの記憶域はプログラムが一般に変えることができないメモリから割当てられる。その後、記憶域がブロック３２６に関連して上に説明されたようにプログラムについて割当てられ、アドレスがＰＣＢ内に保管される。省略値権限を使用するブロック３２８の処理はプログラムのハッシュの計算を含まず、ルーチンはブロック３３４へ分岐して、プログラム実行に備える。

【０１６３】

ブロック３３０に移って、ブロック３２６の計算されたプログラムハッシュがＰＡＩ内に記憶されるハッシュと一致するか否かを決定するチェックが行なわれる。もしハッシュが一致しなければ、ルーチンはブロック３３２へ分岐し、そこで「プログラムＸが変えられた、または損害を受けた。」というようなエラーメッセージが呼出プログラムへ送られ、ルーチンはブロック４１０へ分岐し、プログラムの実行を抑制する。

【０１６４】

ブロック３３４において、ハッシュが一致すると決定された後、またはブロック３２８における処理の後、プログラムが初期実行のために用意される。初期実行のための用意は、初期状態のセット、およびプログラムのＰＣＢにおける情報の「再開」を含み、それによってプログラムは適切なエントリポイントで開始するであろう。さらに、プログラムのＰＣＢは実行スタックの先頭に置かれるであろう。

【０１６５】

図１５へ移り、ブロック３３６において、実行スタックの先頭に置かれると、現在のプログラムは実行を開始するか、または再開する。ブロック３３０ないし４１０で起きる処理は、プログラムを実行するために慣用的に行なわれる動作を含む。処理動作がこれよりＰＡＩ処理を含むそれらの動作に重点をおいて説明されるであろう。ブロック３３６において、スーパバイザは保管された「再開」点で、様々なレジスタの状態を再ロード（またはロード）して、プログラムが最後に中断された（または初期化された）時までにその点でそれらの状態を示すことによって、プログラムを継続する用意をする。さらに、たとえばスタックポインタなどのようなシステム状態情報が使用されている特定のシステム環境によって回復される。

【０１６６】

ブロック３３６の処理の後、もしアプリケーションプログラムが実行されていると、システムは「スーパバイザ」モードから「隔離（isolation)」モードへ切換え、それによってプログラムは隔離モードで実行を再開する（３３８）。隔離モードにおいて、プログラムは「スーパバイザ」モードへコンピュータを切換えて戻す保護されたスーパバイザ呼出を介して以外はコンピュータ資源に影響を及ぼすことができない（或る場合、および或る環境において、プログラムが「スーパバイザ」モードで実行するように設計され、要求されることが可能であろうことが注目される。この場合、プログラムがそのＰＡＩで規定されるように適切に権限付与されると仮定すれば、或る点において「スーパバイザ」機能を使用し、「スーパバイザ」状態動作が可能なようにそのＰＣＢの状態をセットするであろう。このような場合、その状態をチェックし、もしセットしてあれば、プログラムスーパバイザ状態へ制御を与えることが適当であろう。）。

【０１６７】

ブロック３４０において、プログラムが制御された「スーパバイザ」機能を要求していることが推定される。このような環境下で、たとえば予め定められた状態ワー

ドをセットすることによってコンピュータを「スーパバイザ」モードへ切換え、保護されたシステム監視中断ルーチンへ制御を送る。プログラムの再開位置はプログラムのＰＣＢに保管され、他の適切なシステム状態はＰＣＢに保管される。その後、アクセスされるべき機能および資源が決定され、アクセスの性質は、たとえば読出、変更、および削除などである。

【０１６８】

さらに、ブロック３４０において、プロセス制御ブロックに記憶されるＰＡＩ情報から調査が行なわれる。ブロック３４０の処理を補うため、またはそれに関連して、ブロック３４２において調査されたＰＡＩが要求された資源へのアクセスを許容されたか、または要求された機能を行なうことを許容されたかを決定するチェックが行なわれる。たとえば、もし電子郵便を使用することが試みられるならば、プログラムが電子郵便機能を行なう権限を付与されたか否か、もしそうであれば、郵便が１組の郵便識別子に制限されるか否かを決定するチェックがＰＡＩから行なわれる。

【０１６９】

もし３４２のチェックで、ＰＡＩが試みられた機能、または資源のアクセスを許容しないということを明示すれば、ブロック３４４でプログラムがその制限を超えることを試みているということを示すエラーメッセージが生成され、資源または機能へのアクセスが否定され、適当なエラーコード、またはメッセージが生成される。ブロック３５０において、アクセスの達成を試みているプログラムが、アクセスを否定されているということを知らされるべきか否かを決定するチェックが行なわれる（３５０）。もしブロック３５０のチェックで、プログラムがそう知らされるべきであると明示されれば、ブロック３５２においてプログラムがその要求がうまく行なわれず、かつ抑制されるようにせしめたアクセス侵害の型を示すメッセージとともに実行を再開することが許容される。ルーチンはプログラムの実行を再開するためにブロック３３６へ分岐して戻る。このような環境下でプログラムは、たとえばそのＰＡＩが特定のファイルについて権限を読出す権限のみが与えられているということを知らされてもよく、一方でそのファイルへ書込む試みが行なわれた。もしブロック３５０のチェックが、呼出プログラムが知らされるべきでないと示せば、適当な状態および関連のメッセージ（呼出プログラムのための）が生成され、特定されないアクセス侵害による終了を示す３５６。

【０１７０】

もしブロック３４２のチェックが、ＰＡＩが機能または資源へのアクセスを許容すると明示すれば、ブロック３４６で、慣用的なアクセス制御を与え、プログラムのユーザがまだ自分の権限の境界内にあることを確実にするためのチェックが行なわれる。このチェックは、機能

または資源の要求がこの特定のユーザのためのシステムによって許容されるものの範囲内であることを確実にする。したがって、ＰＡＩはプログラムが或るクラスのファイルにアクセスすることを許容するであろうが、特定のユーザに関するセキュリティレベルがそのようなファイルへのそのユーザのアクセスを許容しないかもしれない。ブロック３４６は従来のセキュリティ技術を適用して権限を適切に付与されないユーザからシステムを保護する。このチェックはたとえば、署名すると最初にシステム内に入るユーザ識別コードに基づいてもよい。ブロック３４８で示されるように、もしユーザが権限付与されなかったならば、プログラムがユーザのアクセス能力を侵害することを試みているので、アクセスが否定され、適切なエラーコード／メッセージが生成される。その後、ブロック３５０および３５２に関して上に説明された処理が開始される。

【０１７１】

もしユーザがブロック３４６の処理によって定められるように権限付与されれば、ブロック３５４において示されるように機能が行なわれる。もし機能がプログラムの退出であれば、ルーチンはブロック３５８を介してプログラムから退出し、そこで関連のＰＣＢが実行スタックの先頭から取除かれる。

【０１７２】

さらなる終了処理がブロック４１０で行なわれ、そこでプログラムの実行中に蓄積されたいかなる漂遊記憶および資源も解放され、それは必要に応じてプログラムＸに割当てられた記憶およびそのＰＡＩ記憶を含む。ＰＣＢおよびすべての関連の記憶が解放され、エラーコードおよびメッセージを適切に含む最終状態情報がプログラムの呼出人に提示される。その後、ルーチンはブロック３３６へ分岐して戻り呼出プログラムを再開する。

【０１７３】

最後に、ブロック３５４へ戻って、もしプログラムの呼出が行なわれるべき機能であれば、ルーチンは図１４のブロック３００へ分岐し、適切なプログラムを呼出す。

【０１７４】

この発明は現在最も実際的、かつ好ましい実施例であると考えられるものに関して説明されてきたが、この発明は開示される実施例に限定されるべきではないと理解されるべきであり、前掲の請求項の精神および範囲内に含まれる様々な変更および同等の配置を包括することが意図される。

【図面の簡単な説明】

【図１】　この発明と関連して使用され得る例証的なコミュニケーションシステムを示すブロック図形式の図である。

【図２】　プログラム権限情報の例示の図である。

【図３】　プログラム権限情報をプログラムに関連づけ

る例証的な方法を例示する図である。

【図４】　プログラム権限情報をプログラムに関連づける例証的な方法を例示する図である。

【図５】　プログラム権限情報をプログラムに関連づける例証的な方法を例示する図である。

【図６】　プログラム権限情報をプログラムに関連づける例証的な方法を例示する図である。

【図７】　不明の出所のプログラムと関連して、ユーザがこの発明をどのように使用し得るかを例示する一般的なフローチャートの図である。

【図８】　この発明の例証的な実施例に従うプログラムコントロールブロックデータ構造の例示の図である。

【図９】　プログラム権限情報を確立するためのプログラムの動作のシーケンスを正確に叙述するフローチャートの図である。

【図１０】　プログラム権限情報を確立するためのプログラムの動作のシーケンスを正確に叙述するフローチャートの図である。

【図１１】　プログラム権限情報を確立するためのプログラムの動作のシーケンスを正確に叙述するフローチャートの図である。

【図１２】　プログラム権限情報を確立するためのプログラムの動作のシーケンスを正確に叙述するフローチャートの図である。

【図１３】　プログラム権限情報を確立するためのプログラムの動作のシーケンスを正確に叙述するフローチャートの図である。

【図１４】　プログラム権限情報を処理する際のスーパバイザプログラムによって実行される動作のシーケンスを例示する図である。

【図１５】　プログラム権限情報を処理する際のスーパバイザプログラムによって実行される動作のシーケンスを例示する図である。

【符号の説明】

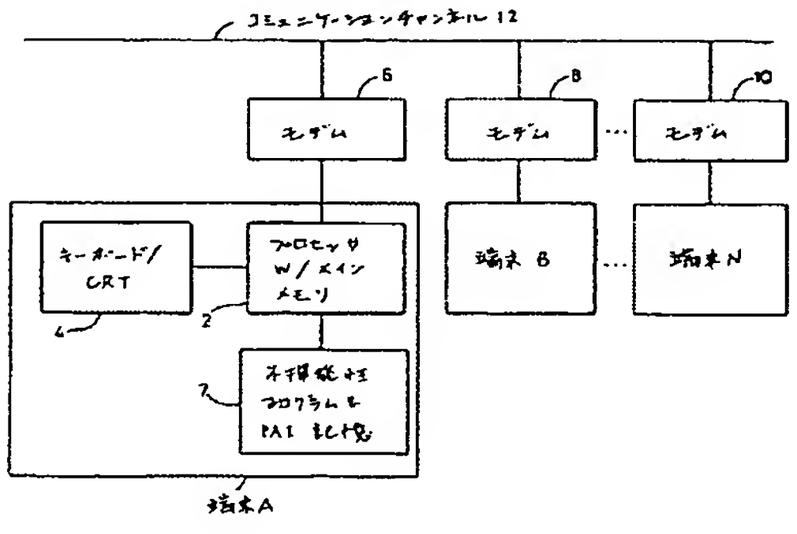
２　プロセッサ

４　ディスプレイ

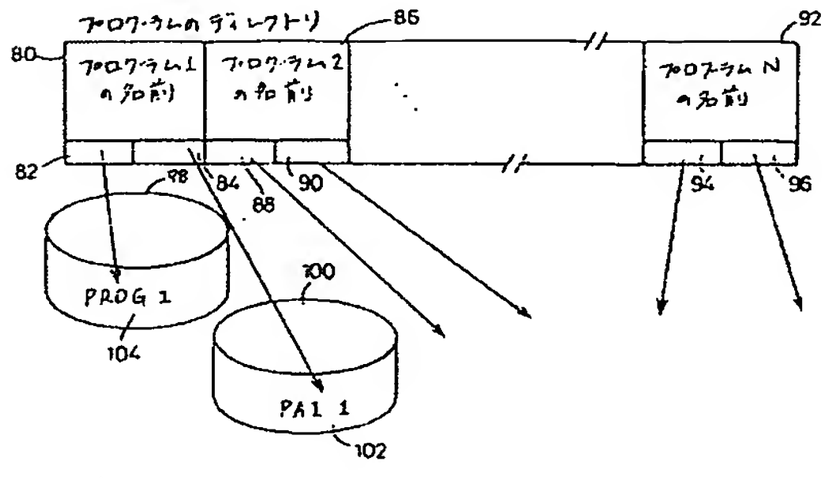
７　メモリ

１２　コミュニケーションチャンネル

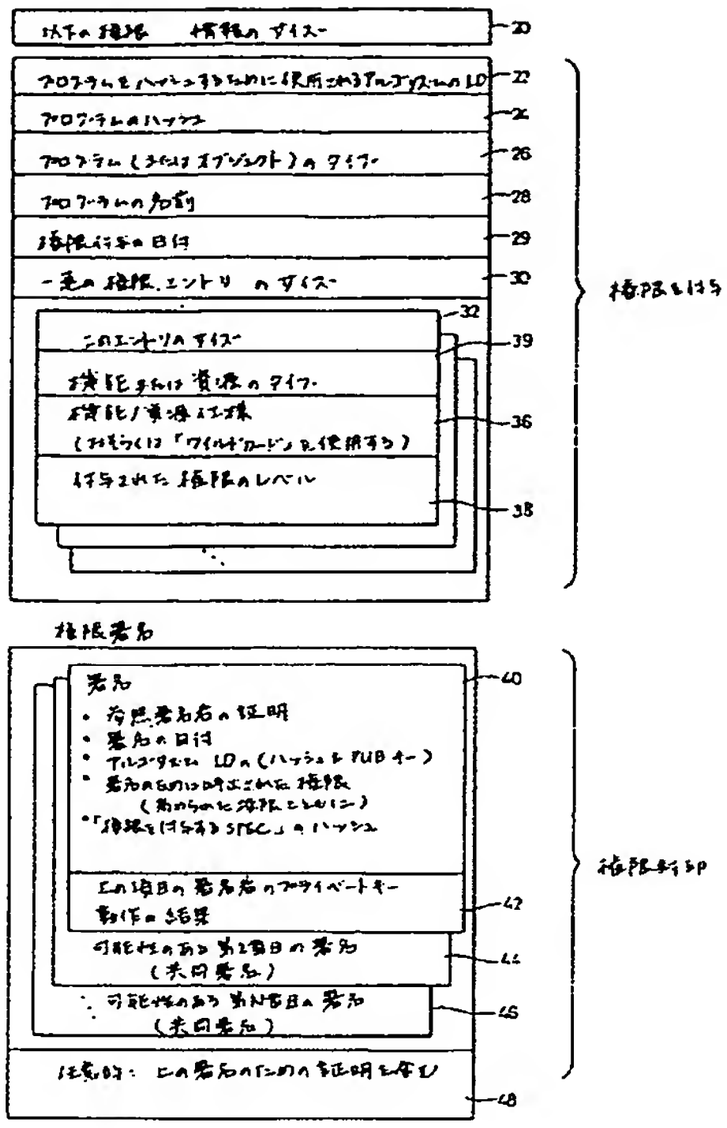
【図１】



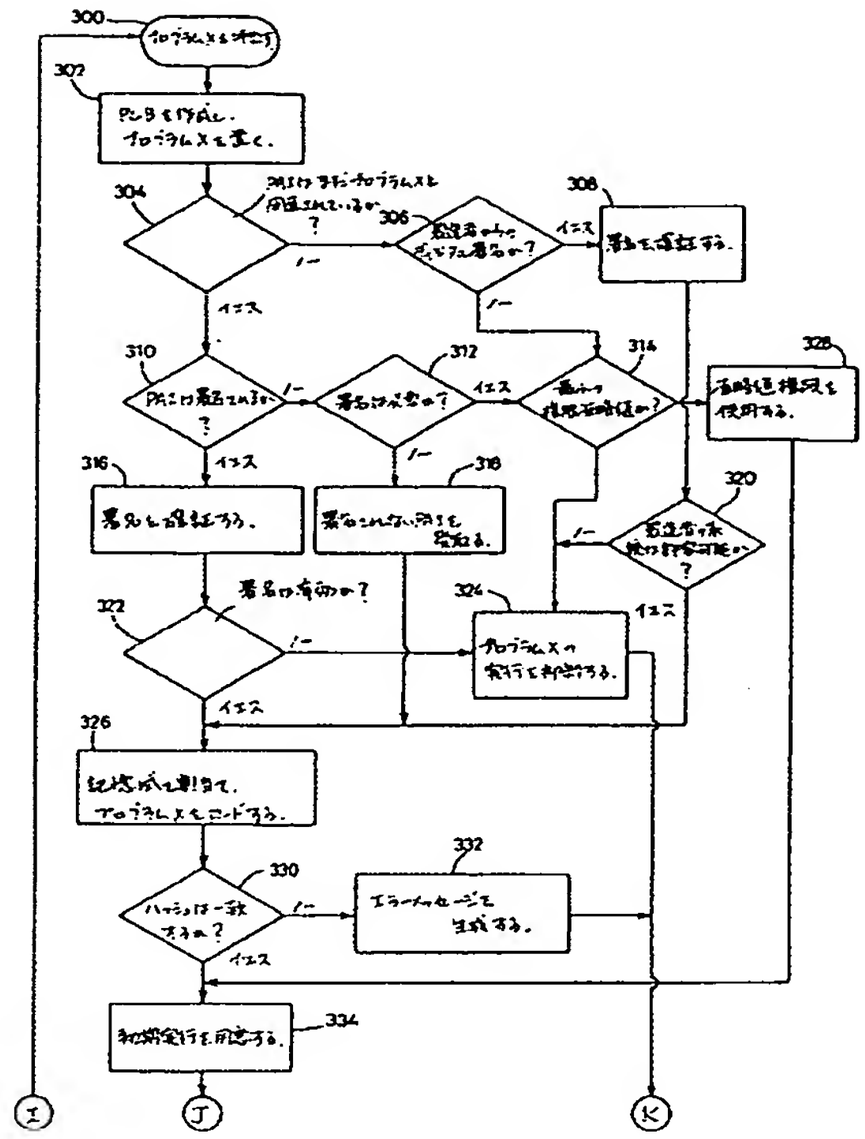
【図３】



【図２】

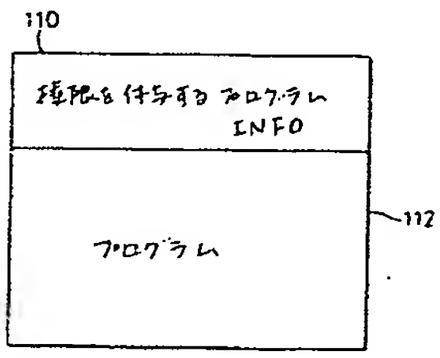


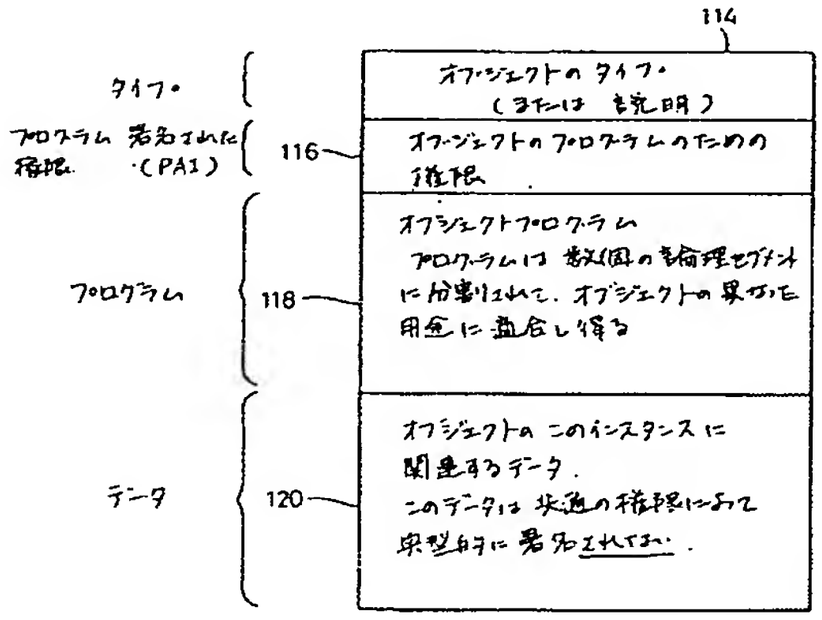
【図１４】



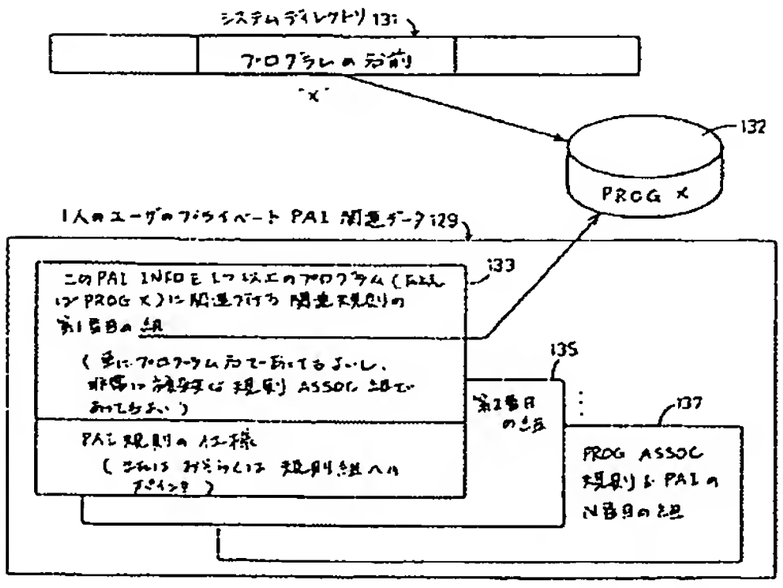
【図４】

【図５】

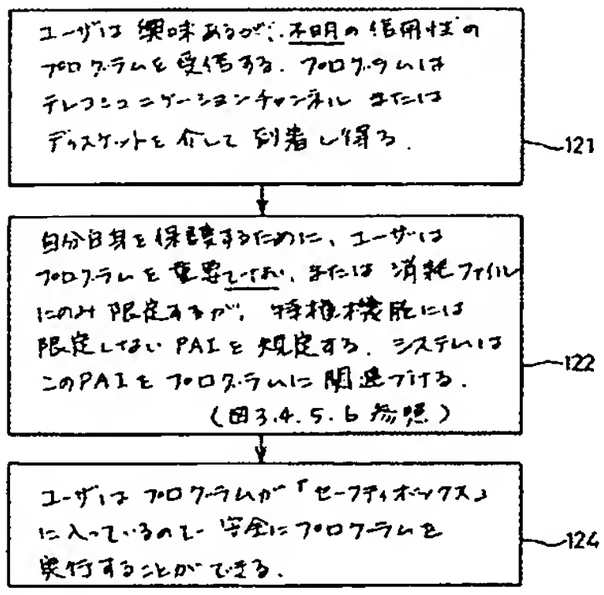




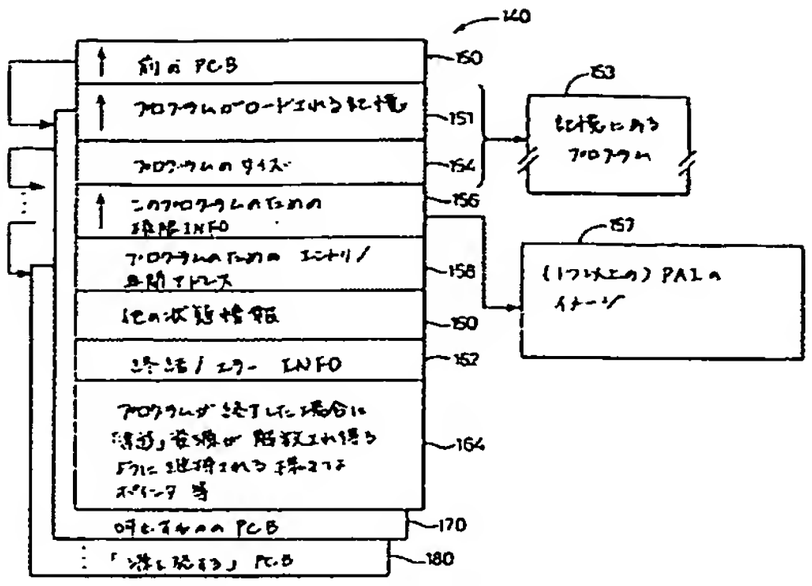
【図６】



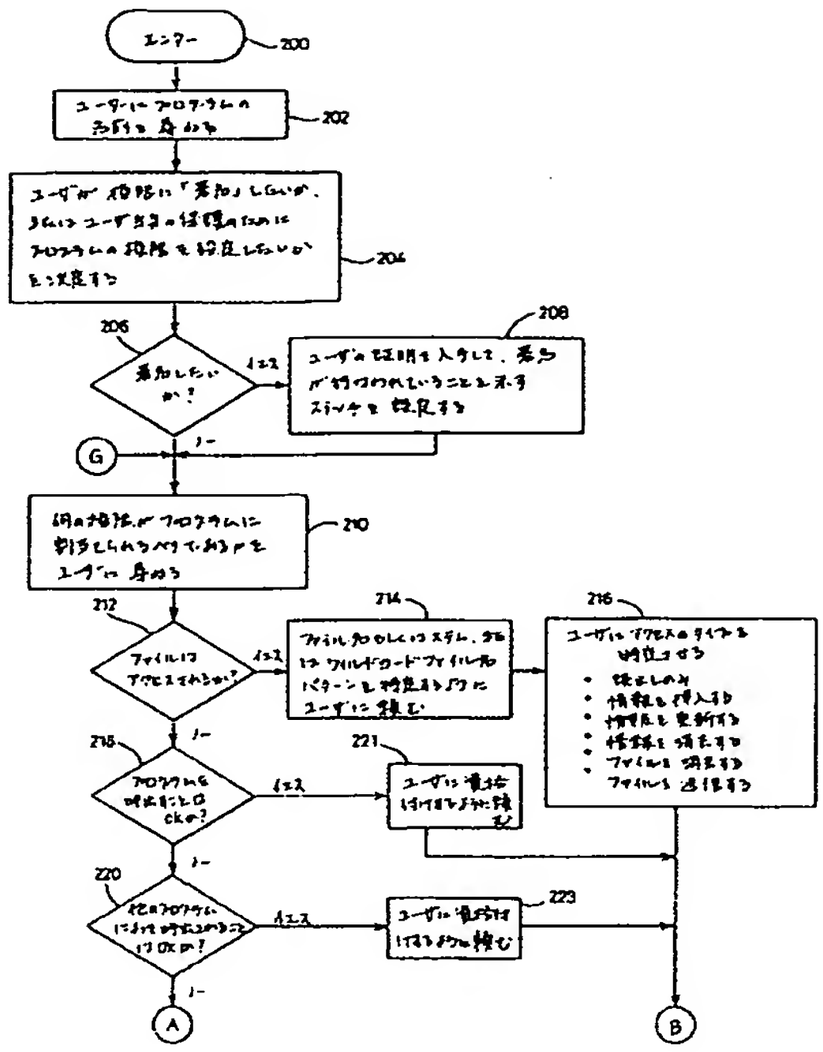
【図７】



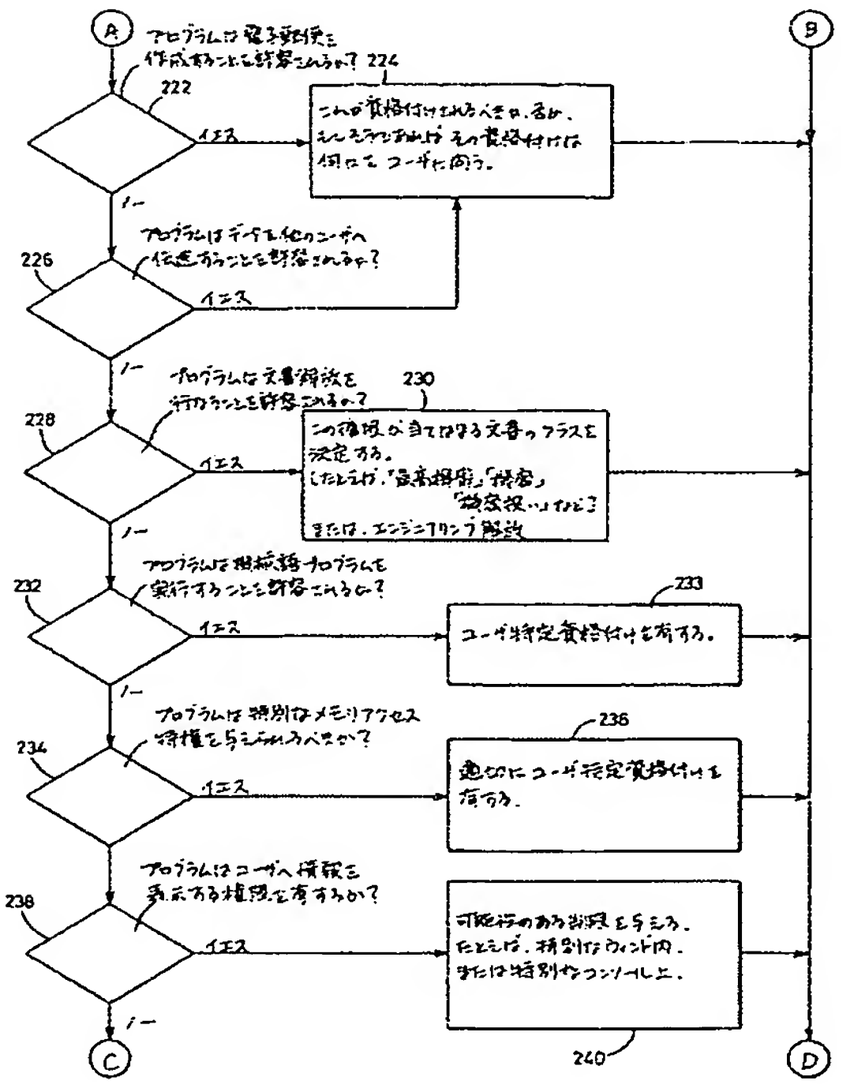
【図８】


140
前の PCB
150
プログラムがロードされる位置
151
プログラムのサイズ
154
このプログラムのための状態INFO
156
プログラムのためのエントリ/開始アドレス
158
他の状態情報
160
終了/エラー INFO
162
プログラムが終了した場合に「通知」要求が処理されるドアに進行される保護フラグ等
164
呼出すもののPCB
170
「後を続ける」PCB
180
153
状態にある プログラム
157
(1つ以上の) PALの イメージ

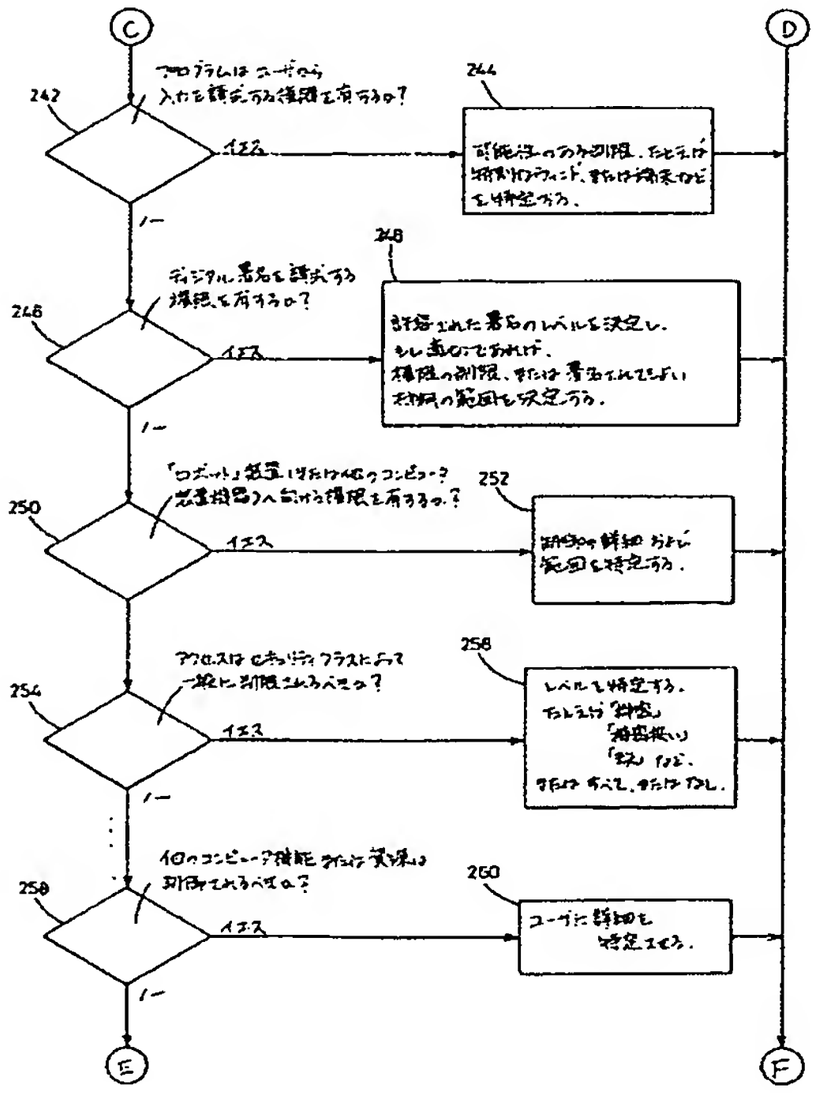
【図９】


エンター
200
ユーザーにプログラムの実行を要求
202
ユーザが現時に「参加」しないが、さもユーザ自身の処理のためにプログラムの処理を特定しないかと決定する
204
参加したいか?
206
イエス
ユーザの証明を入力して、参加が許可されていることを示すシンボルを検索する
208
G
次の処理がプログラムに割当てられるべきであるかをユーザに要求
210
ファイルにアクセスするか?
212
イエス
ファイル知りたいシステム、または ワイルドカードファイルネームパターンを特定するようにユーザに強む
214
ユーザはアクセスのタイプを特定する
• 読出しのみ
• 情報を挿入する
• 情報を更新する
• 情報を消去する
• ファイルを開ける
• ファイルを作成する
216
プログラムを呼出すためのOKか?
218
イエス
ユーザの資格付けを決定するために強む
221
次のプログラムにおいて呼出すためのOKか?
220
イエス
ユーザに資格付けを決定するために強む
223
A
B

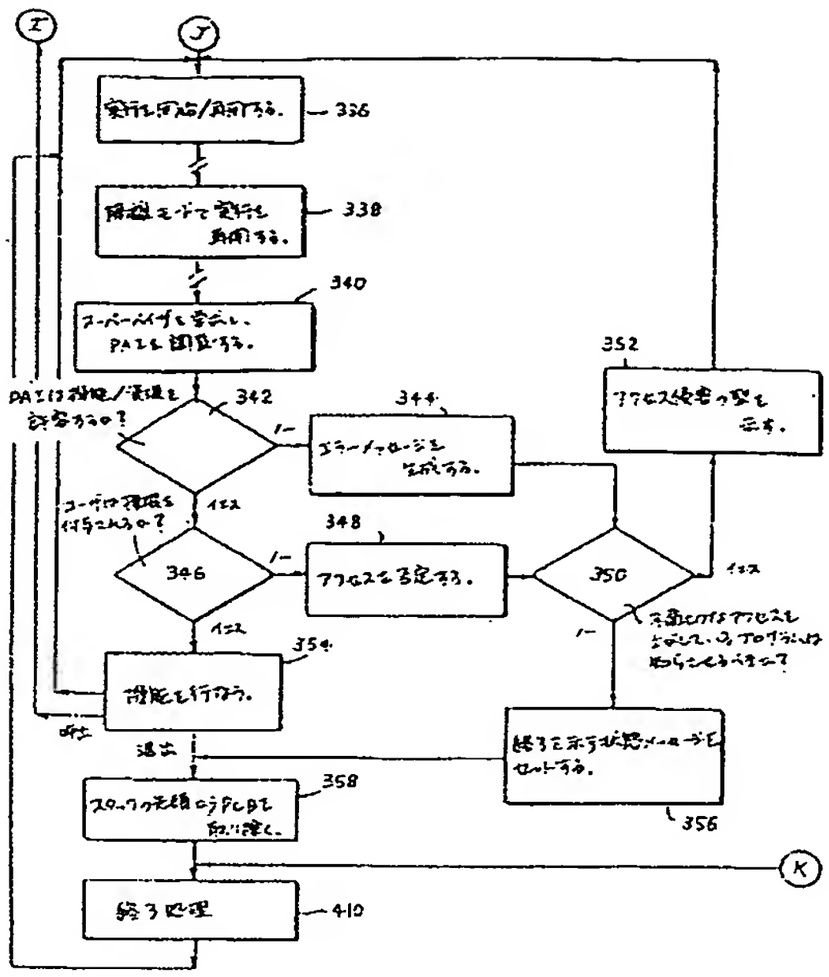
【図１０】


A
プログラムは電子署名を作成するために許容されるか?
222
イエス
これが資格付けされるべきか、否か、もしそうであれば その資格付けは何にもユーザに向う。
224
ノー
プログラムはデータを他のユーザへ伝送することを許容されるか?
226
イエス
ノー
プログラムは文書解放を行なうことを許容されるか?
228
イエス
この権限が当てはまる文書のクラスを決定する。
したとえば、「営業提案」「提案」「秘密提示」など
または、エンジニアリング解放
230
ノー
プログラムは機械語プログラムを実行することを許容されるか?
232
イエス
ユーザ特定資格付けを有する。
233
ノー
プログラムは特別なメモリアクセス特権を与えられるべきか?
234
イエス
適切にユーザ特定資格付けを有する。
236
ノー
プログラムはユーザへ情報を表示する権限を有するか?
238
イエス
可能性のある制限を与える。
たとえば、特別なウィンドウ内、または特別なコンソール上。
240
ノー
B
C
D

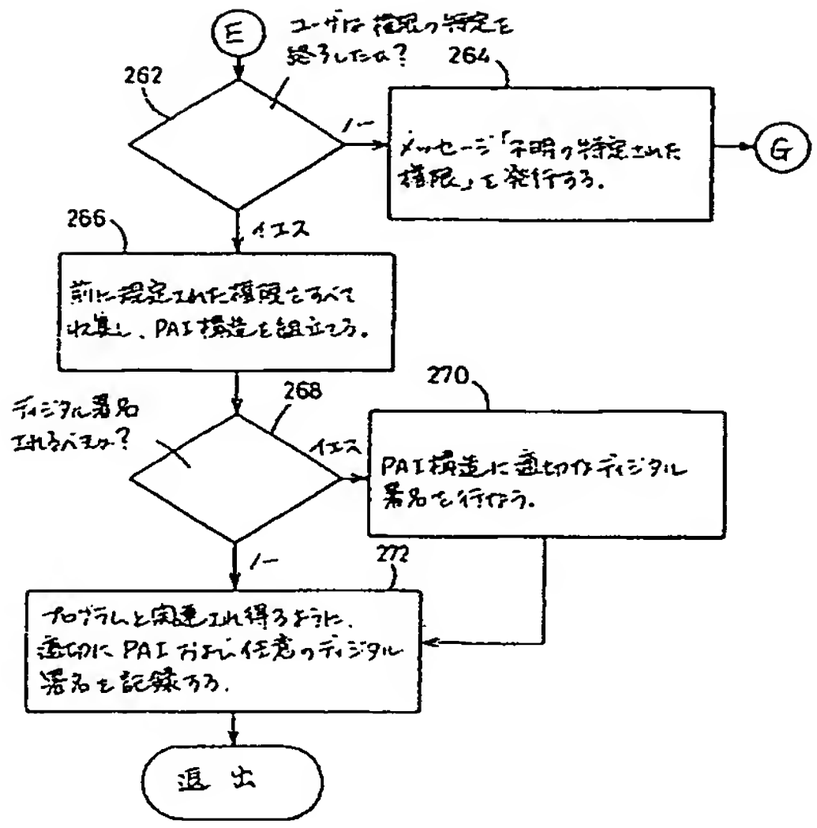
【図１１】


C
プログラムはユーザから入力を要求する権限を有するか?
242
イエス
可能性のあるクラス制限、たとえば特別なフィールド、または検索などを特定する。
244
ノー
ディジタル署名を要求する権限を有するか?
246
イエス
許容された署名のレベルを決定し、もし適切であれば、権限の制限、または署名されてよい対象の範囲も決定する。
248
ノー
「ロボット」装置にはたらくコンピュータ支援機器へ向かう権限を有するか?
250
イエス
許容の詳細 および範囲を特定する。
252
ノー
アクセスはセキュリティクラスによって一般に制限されるべきか?
254
イエス
レベルを特定する。
たとえば「秘密」「特定扱い」「なし」など。
すべて、または なし。
258
ノー
1回のコンピュータ技能 または資格は制御されるべきか?
258
イエス
ユーザに詳細を特定させる。
260
ノー
E
F

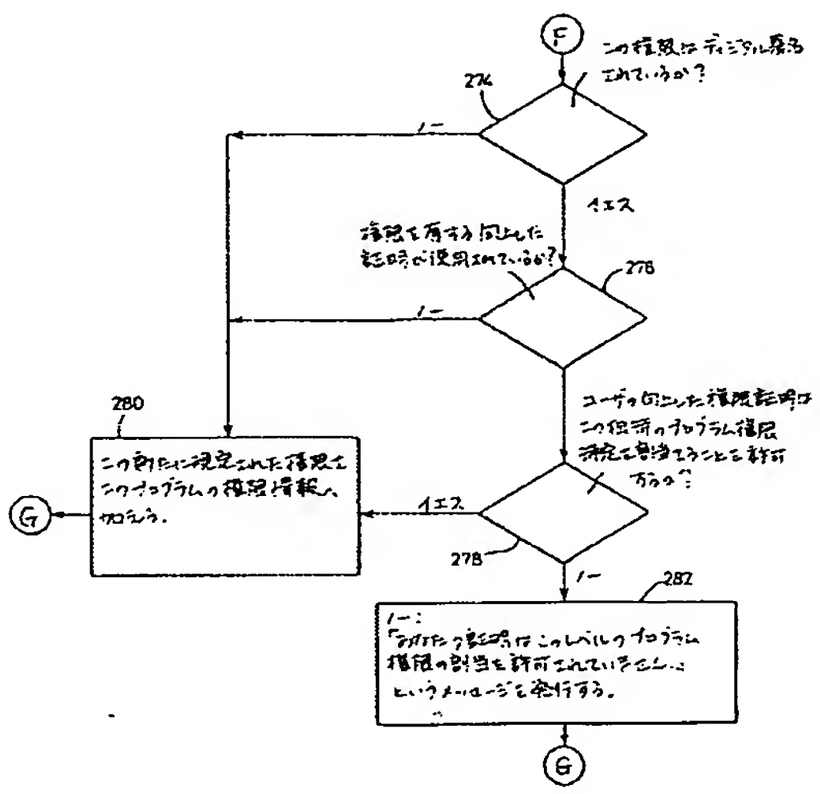
【図１５】


I
J
実行を開始/再開する。
336
指定モードで実行を再開する。
338
スーパーバイザを呼び出し、PAIを回復する。
340
PAIは指定/要求を許容するか?
342
エラーメッセージを生成する。
344
アクセス違反の数を示す。
352
ユーザは権限を付与したか?
346
アクセスを拒否する。
348
イエス
ノー
機能を行なう。
354
終了
退出
終了を示す状態メッセージをセットする。
356
スタックの先頭のプログラムを取り除く。
358
K
終了処理
410

【図１２】


E
ユーザは権限の特定を終了したか?
262
264
ノー
メッセージ「不明な特定された権限」を発行する。
G
イエス
266
前に指定された権限をすべて収集し、PAI構造を組立てる。
ディジタル署名されるべきか?
268
270
イエス
PAI構造に適切なディジタル署名を行なう。
ノー
272
プログラムと関連し得るように、適切にPAIおよび任意のディジタル署名を記録する。
退出

【図１３】


F
この権限はディジタル署名されているか?
274
ノー
イエス
権限を有する同じた話時が使用されているか?
278
ノー
280
この前に指定された権限とこのプログラムの権限情報へ加える。
G
イエス
ユーザがこの権限話時にこの任務のプログラム権限指定を割当てることを許可するか?
278
ノー
282
ノー:
「ユーザは話時はこのレベルのプログラム権限の割当を許可されていません」というメッセージを発行する。
G

フロントページの続き

(72)発明者　アディソン・エム・フィッシャー
アメリカ合衆国、３３９４２　フロリダ州、ナプルズ、フォーティーンス・アベニュ・サウス、６０

合議体
審判長　井関　守三
審判官　堀江　義隆
審判官　冨吉　伸弥

(56)参考文献　特開平４－１２３２５０（ＪＰ，Ａ）
米国特許第５００５２００（ＵＳ，Ａ）
スタンフォード・ディール、外３名著，”データ保護のための処方箋”，日経バイト，日本，日経ＢＰ社，１９９１年１０月１日，第９１号，ｐ．３５１－３６９

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　9/06
H04L　9/00